Administrator’s Guide for Absolute Agents, Revision 21

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

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

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

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

©2017-2020 Absolute Software Corporation. All rights reserved. Reproduction or transmission in whole or in part, in any form, or by any means (electronic, mechanical, or otherwise) is prohibited without the prior written consent of the copyright owner. ABSOLUTE, the ABSOLUTE logo, and PERSISTENCE are registered trademarks of Absolute Software Corporation. Other names or logos mentioned herein may be the trademarks of Absolute or their respective owners.
**Contents**

Chapter 1: Introduction ........................................................................................................ 6

About this guide .................................................................................................................. 6
  Audience .......................................................................................................................... 6
  Using this guide ................................................................................................................ 6

About the agent .................................................................................................................. 6

Contacting Absolute Technical Support ............................................................................ 7

Chapter 2: Installing and managing the agent on Windows devices ................................. 8

Device compatibility .......................................................................................................... 8
  Firmware persistence ....................................................................................................... 9
  Compatibility with Microsoft BitLocker® Drive Encryption ............................................ 9
  Compatibility with other full-disk encryption products .................................................. 9
  File List and Remote File Retrieval ............................................................................... 9
  Real-Time Technology requirements ............................................................................ 9

Downloading and installing the agent on an individual device ......................................... 10
  Before you begin ............................................................................................................ 11
  Downloading the Installer ............................................................................................ 11
  Installing the agent on an individual device ................................................................. 12
  Verifying the agent installation .................................................................................... 13

Installing the agent on multiple devices ........................................................................... 15
  Deploying the agent using disk imaging ...................................................................... 15
  Deploying the agent using SCCM ................................................................................ 16
  Deploying the agent using Active Directory ................................................................. 16

Managing the agent .......................................................................................................... 16
  Starting the Agent Management utility ....................................................................... 16
  Viewing agent call details ............................................................................................ 16
  Forcing a call to the Monitoring Center ...................................................................... 17
  Configuring IP proxy settings ...................................................................................... 17
  Upgrading the agent on Windows devices .................................................................. 18
  Removing the agent from Windows devices ............................................................... 18

Chapter 3: Installing and managing the agent on Mac devices ....................................... 19

Device compatibility .......................................................................................................... 19

Downloading and installing the agent on an individual device ......................................... 19
  Before you begin ............................................................................................................ 20
  Downloading the Installer ............................................................................................ 20
  Installing the agent on an individual device ................................................................. 21
  Verifying the agent installation .................................................................................... 22
Chapter 4: Installing and managing the agent on Android devices

Device compatibility

Downloading and installing the Absolute Agent for Android

Before you begin

Managing the agent using the Absolute Dashboard

Setting your password on first use

Changing your password

Viewing agent status information

Viewing the Device State service

Viewing the agent Logs

Forcing a test call to the Monitoring Center

Sending diagnostic information to Absolute Technical Support

Upgrading the agent

Removing the agent

Chapter 5: Deploying and managing the Chromebook extension

Device compatibility

Configuring and deploying the Chromebook extension

Before you begin

Adding your Google account to Absolute

Configuring settings in the Google Admin Console

Deploying the Chromebook extension to users

Configuring the Stolen OU

Managing your Google account details in the Absolute console

Editing Google account details

Deleting a Google account

Unenrolling Chromebooks

Deprovisioning Chromebooks

Moving the device to an unsynced OU

Deselecting the device’s OU

Using the Unenroll Device action
Removing the Chromebook extension ................................................................. 50
  Removing the Chromebook extension from all devices in an OU ............................... 51
  Removing the Chromebook extension from specific users ........................................ 51

Chapter 6: Testing network connectivity using the Network Diagnostics Tool .................. 52
  Downloading the Absolute Network Diagnostics Tool ............................................. 52
  Using the Network Diagnostics Tool ....................................................................... 52
  Viewing the Network Diagnostics log file .................................................................. 53
Chapter 1: Introduction

The Absolute® agent is the part of Absolute’s technology that resides on managed devices. After the agent is initially installed on a device, the agent is activated with the device’s first call to the Monitoring Center. During this activation call, the Monitoring Center assigns a unique Identifier to the device and creates an inventory record that contains details about the device’s identification points in a database.

This chapter provides information about the agent and how to contact Absolute Technical Support.

About this guide

The Administrator’s Guide for Absolute Agents provides instructions on how to install and manage the agent on Windows, Mac, and Android devices. It also provides instructions on how to install and manage the Absolute for Chromebooks extension on Chromebook devices.

Audience

This guide is written primarily for users in the Administrator role in the Absolute console who perform agent management tasks, such as downloading Installer packages, installing the agent on devices, and managing the agent in various ways.

Using this guide

The Administrator’s Guide for Absolute Agents for Absolute includes the following chapters:

- **Introduction** (this chapter) provides an overview about this guide for use with Absolute.
- **Installing and managing the agent on Windows devices** provides information about how to install the agent on individual and multiple Windows devices, and how to manage the agent.
- **Installing and managing the agent on Mac devices** provides information about how to install the agent on individual and multiple Mac devices, and how to manage the agent.
- **Installing and managing the agent on Android devices** provides information about how to install the agent on Android devices and how to manage the agent.
- **Deploying and managing the Chromebook extension** provides information about how to download and install the Absolute for Chromebooks Extension on Chromebook devices, and how to manage the extension.
- **Testing network connectivity using the Network Diagnostics Tool** provides information about how to test your devices’ ability to connect to the Absolute Monitoring Center.
- **Glossary** provides a list of commonly used terms and their definitions, and acronyms that are related to this guide.

About the agent

The Absolute agents are client software that you install on devices you want to manage using Absolute services. When installation is complete, the agent on each device contacts the Monitoring Center to obtain a unique Identifier for that device.
The agent continues to contact the Monitoring Center on a regular basis to report its location. Communication between the agent and the Monitoring Center is quick, silent, and requires no input from you.

The agent remains concealed on your device, and it does not affect system performance or interfere with Internet activities.

**NOTE** On certain makes and models, the agent needs to contact the Monitoring Center twice to complete activation.

### Contacting Absolute Technical Support

If you have difficulty using or installing the agent, submit a Support case by logging in to the Absolute console, clicking on the navigation bar, and then clicking **Support**. For more information about completing the case submittal form, see *Contacting Technical Support* in the online Help.

You can also contact Absolute Technical Support at [www.absolute.com/support](http://www.absolute.com/support). Follow the on-screen instructions to contact Technical Support for your region. We welcome your questions, comments, and feature requests.
Chapter 2: Installing and managing the agent on Windows devices

This chapter provides information about device compatibility and instructions for installing the agent on Microsoft® Windows devices in the following ways:

- **Direct installation**: used to install the agent on individual devices not connected through a network. This method requires hands-on contact with each target device. For details about this type of installation, see [Downloading and installing the agent on an individual device](#).
- **Batch installation**: used to install the agent on multiple devices. For details about this type of installation, see [Installing the agent on multiple devices](#).

Use the installation method that best suits the prevailing circumstances and your organization’s requirements.

This chapter also includes information about managing your Windows devices. The agent installation package includes the Agent Management utility, which you can use to do the following:

- Verify that the agent is present on a device, and force agent calls for testing and diagnostic purposes.
- Confirm the state of the agent in an image, before deploying the image to multiple devices in your network.

This chapter includes the following sections:

- Device compatibility
  - [Downloading and installing the agent on individual devices](#)
  - [Installing the agent on multiple devices using disk imaging](#)
  - [Managing the agent](#)

### Device compatibility

To ensure that your Windows devices are compatible with the agents, you need to meet the following requirements:

- Supported operating systems:
  - Windows 10
  - Windows 8.1

  **NOTE** Windows RT 8.x is not supported.

  - Windows 7
- Internet connection

If you want to ensure that the agent survives accidental or malicious tampering, confirm that your Windows devices support firmware persistence, which is described next.
Firmware persistence

Firmware persistence support is a type of Persistence® technology provided by Absolute. Most Original Equipment Manufacturers (OEMs) integrate this technology within the computer BIOS or firmware.

To see a list of manufacturers who provide firmware persistence, go to www.absolute.com/bios.

Compatibility with Microsoft BitLocker® Drive Encryption

BitLocker Drive Encryption (BitLocker) is a full-disk encryption feature included in most versions of the Windows operating system. BitLocker is designed to protect data by providing encryption for the operating system drive and fixed data drives.

The agent is compatible with BitLocker. When BitLocker is enabled on a device, it is temporarily suspended when firmware persistence is activated, which occurs during the first agent call after the agent is installed. BitLocker is enabled automatically when the device is restarted. This process is also used when firmware persistence is deactivated, which occurs when the device is unenrolled from your account.

**IMPORTANT** If a user is logged in to a device during activation of firmware persistence, the user sees a message stating that a restart is required. If the user chooses to Postpone the restart and then logs off before the restart occurs, the device restarts after the postpone action's timer runs out. Similarly, if a user is logged in during deactivation of firmware persistence, the user sees the same message.

For more detailed information, see Knowledge Base article 000001587.

Compatibility with other full-disk encryption products

The agent is fully compatible with full-disk, and file and folder encryption products. If you use a full-disk encryption product other than BitLocker, such as McAfee Drive Encryption™, ensure that you install the agent before you install and enable full-disk encryption on the device. For more information, see Knowledge Base article 000001446.

File List and Remote File Retrieval

You can view a list of files from your managed Windows devices and select any essential files you want to retrieve before invoking Device Freeze or Data Delete. Both the File List and Remote File Retrieval features work only on Windows devices, and File List works only on Windows devices on which .NET Framework 2.0 is installed.

Real-Time Technology requirements

Real-Time Technology (RTT) provides further data protection to Windows devices that have an Absolute agent installed and a mobile broadband adapter that supports SMS messaging.

RTT sends managed devices an SMS message through the SMS Gateway and either instructs the devices to perform an action, or initiate an immediate agent call.
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 is running a supported version of the Windows operating system.
- The agent is installed and the device is regularly calling the Monitoring Center.
- The device has a valid mobile data subscription that supports SMS messaging.
- The device has a supported mobile broadband adapter, such as:
  - **Gobi 1000**: an embedded mobile broadband adapter available on UMTS and EvDO networks. Including the following Gobi variants:
    - Qualcomm UNDP-1
    - Qualcomm 9202
    - Dell 5600
    - HP un2400
  - **Gobi 2000**: an embedded mobile broadband adapter available on UMTS and EvDO networks. Including the following Gobi variants:
    - Qualcomm 920b
    - HP un2420
  - **Gobi 3000**: an embedded mobile broadband adapter on Windows 7 only and UMTS and EvDO networks, including the following Gobi variants:
    - Sierra Wireless MC8355 (similar to HP un2430)
    - Dell DW5630 (believed to be made by Novatel Wireless)
    - Option GTM689W
  - **Ericsson F3507**: an embedded UMTS mobile broadband adapter
  - **Ericsson F3607gw**: an embedded UMTS mobile broadband adapter
  - **Ericsson F5521gw**: embedded UMTS mobile broadband adapter and the following variants on Windows 7 only:
    - Dell DW5550
    - HP hs2340
  - **Novatel Wireless mobile broadband adapters** on UMTS and EvDO networks and Novatel Wireless E362 (similar to HP lt2510) on Windows 7 only
  - **Sierra Wireless mobile broadband adapters**: mobile broadband adapters on the UMTS and CDMA/EvDO networks
    - Sierra Wireless UMTS mobile broadband adapters
    - Sierra Wireless MC5720: an embedded CDMA/EvDO mobile broadband adapter
    - Sierra Wireless MC5725: an embedded CDMA/EvDO mobile broadband adapter

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

- An active data plan with SMS support for the mobile broadband adapters.

## Downloading and installing the agent on an individual device

The instructions in this section apply to installing the agent on individual devices, which requires hands-on contact with each target device. This installation method is commonly used to install the agent on new devices that are not connected to a network.

This section includes the following topics:
Before you begin

**IMPORTANT** Follow these instructions to ensure that the agent remains tamper-resistant.

To ensure a trouble-free and secure installation:

- Use a virus-scanning program to ensure that your hardware is free from viruses.
- Ensure the device is connected to the Internet.
- If the device is not using the BIOS agent, ensure that the primary hard drive is listed first in the boot order specified in the BIOS.

**Downloading the Installer**

Before you can install the agent on Windows devices, you need to download the Full Agent Installer zip folder. You can use this installer to deploy the agent package from the command line or the InstallShield wizard.

**IMPORTANT** Where the version and account numbers are included in a filename, the convention used shows up to four digits `<n>.<n>.<n>.<n>`, which indicates a release number of up to four digits, and then a hyphen and your customer account identifier; for example, `7.2.0.1-4757.zip`. This convention holds true for both the .exe and .msi files. For the purposes of illustration, this guide will show the version number using two digits.

The extracted agent installation package includes the following key components:

- The `ctmweb` folder, which contains the `ctmweb.exe` and `ctmweb.xsl` files.
- `AbsoluteAgent<n>.<n>-<account_id>.exe` file: the Full Agent Installer in an executable file format, which is used if you want to view the user interface in a language other than English.
- `AbsoluteAgent<n>.<n>-<account_id>.msi` file: for MSI deployment of the Full Agent Installer in the Windows Installer package format.
- A `readme.txt` file that includes the Agent release notes for the current release, in all translated languages supported in the Absolute console.

**To download the agent installer from the Absolute console:**

1. Log in to the Absolute console as an Administrator with Manage permissions for Version Control and Perform permissions for Agent Installer.
2. On the navigation bar, click **Agent Management**.
3. On the Agent Management page next to the agent version that you want to download, click **Download Full Agent Installer**.
4. On the Download Full Agent Installer dialog, do one of the following:

   - If you have never generated a package for this agent version:
     a. Next to Microsoft Windows click the **Generate package** link to generate this agent package. A confirmation message opens. In the background the system processes your request and generates an agent package for your account. This process could take a few minutes.
b. Click **Close** to close the message dialog.

c. On the Agent Management page next to the agent version you generated, click ✅ and click the **Download Full Agent Installer** again.

d. On the Download Full Agent Installer dialog, do one of the following depending on whether the agent package is generated:
   - If the agent package is generated, click the **Download package** link. The zipped agent package is downloaded, which may take a few minutes. (When it's ready, look at the bottom left side of the page to see it.)
   - If the agent package generation process is not yet complete, click ✗ to close the dialog, wait a few minutes, and try again in a few minutes.
   - If the agent package failed to generate, click ✗ to close the dialog and try again or contact Absolute Technical Support.

   • If you have generated a package for this agent version before, click the **Download package** link. The zipped agent package is downloaded, which could take a few minutes.

5. Depending on your browser and operating system, you may need to click through several dialogs to **Save** the .zip folder that includes the installation files to a location of your choice; for example, to the root folder for command line installations. When the download completes, click **Open**.

6. From the location where you just saved the .zip folder, extract its contents to a local folder, a network drive, or to removable media such as a USB device.

   You must extract the entire contents of the **ctmweb** folder in the original Windows zip file you downloaded from the Absolute console. You can copy the files to a hard drive or run them from a USB key or network drive. Make sure these files are in the same directory location as they all work together.

## Installing the agent on an individual device

You can use the command line or the InstallShield wizard to install the agent on a Windows device.

**NOTE** You must have Administrator privileges to install the agent.

## Installing the agent using the command line

Using the command line to silently install the agent on a Windows device eliminates the need to respond to prompts in the InstallShield wizard.

> **To install the agent using the command line:**

1. Open a Command Prompt window as an administrator. For example:
   - Click **Start** and type **cmd**.
   - Right-click **cmd** or **Command Prompt**, and then click **Run as administrator**.
   - On the User Access Control dialog, click **Yes**. The Administrator: Command Prompt window opens. For information about other ways to open a Command Prompt window as an administrator, refer to Windows documentation.

2. Navigate to the appropriate Installer file that you extracted in the task Download the Installer.

3. Do one of the following:
   - To run the MSI Installer:
     - In silent mode, type:
       ```
       msiexec.exe -i AbsoluteAgent<n>.<n>-<account_id>.msi /quiet
       ```
o Specify the installation log by running this command line:

```
msiexec.exe -i AbsoluteAgent<n>.<n>-<account_id>.msi /L*v path_to_log
```

- To run the executable file:
  - In silent mode, type:
    
    ```
    AbsoluteAgent<n>.<n>-<account_id>.exe /S /v/qn
    ```

### Installing the agent using the InstallShield wizard

**NOTE** If you are using the MSI Installer to install the agent on a Windows 10 device, follow the steps in Using the command line.

ToDate install the agent on a device using the InstallShield wizard:

1. Navigate to the appropriate Installer file that you extracted in the task Downloading the Installer.
2. Right-click the Installer file and click Run as administrator. The InstallShield wizard opens.

**NOTE** If the Run as administrator option is not available in the right-click menu, follow the steps in Using the command line to install the agent.

3. If the User Account Control dialog shows, click Yes to permit the install file to be installed.
4. If you are using the Installer in executable file format (AbsoluteAgent<n>.<n>-<account_id>.exe), select your preferred language for the InstallShield wizard and click OK.
5. Click Next and then click Install to start the installation.
6. Click Finish to complete the agent install and exit the InstallShield wizard.

Now you can verify the installation of the agent on your Windows device, as instructed in the next section.

### Verifying the agent installation

You can verify that the agent was installed successfully on your devices in the following ways:

- Using the Agent Management utility
- Using the Absolute console

### Using the Agent Management utility

You can verify that an agent is activated and calling in successfully using the Agent Management utility.

ToDate verify the agent using the Agent Management utility:

1. Ensure that the device is connected to the Internet.
2. Open the Agent Management utility:
   a. Browse to the folder that contains the extracted agent installation package.
   b. Double-click ctmweb.exe to open the Agent Management utility with the CTMWeb Login page active.

**NOTE** If the User Account Control dialog shows, click Yes to permit access to your system.
c. In the **Please enter your password** field, type **password**, which is the default administrative password.
d. Click **Next**.

3. On the Agent Status page, click the **Test Call** tab and click **Start** to force a call.
   
   You should see that the UI is refreshing and, when complete, the result should come back as **Last call successful**, however one of the following may occur:
   
   - If you see a **DL_NA** message, it means that the agent is not present.
   - If you consistently get a **last call failed** message, contact your Absolute representative.

4. To verify that the agent is installed successfully, review these fields:
   
   - **Agent Mode**—confirm that the value is **Active**.
   - **ESN**—Electronic Serial Number, which is also referred to as the unique Identifier. For activated agents, the last four characters of this Identifier are greater than 0000. If the last four characters are 0000, click the **Test Call** tab in the Agent Management utility, and then click **Start** to force a test call to the Monitoring Center. The **Call Status** shows on screen.
   
   - **Last IP Call Date/Time**—shows the appropriate time and date value, indicating a successful call.

   **IMPORTANT** If the **Last IP Call Date/Time** field reads **No last call**, your device failed to contact the Monitoring Center. When the agent call is in progress or your device is not connected to a network, this field shows a question mark (?) .

   - **Last Modem Call Date/Time**—disregard this field; its use was deprecated.

Default settings apply during the agent installation. After installation, you can change the agent settings for individual devices locally using the Agent Management utility. For full details about using the Agent Management utility, see [Managing the agent](#).

If you require further assistance, contact [Absolute Technical Support](#).

If your installation failed, you can force a call and verify its success. See [Forcing a call to the Monitoring Center](#).

### Using the Absolute console

You can verify that an agent is activated and calling in successfully by looking for the device on the Activation Report.

⇒ **To verify the agent installation using the console:**

1. Log in to the Absolute console as an Administrator.
2. On the navigation bar, click 🗄.
3. Click **Go to the Classic Reports page** at the bottom of the page.
4. Under Call History and Loss Control, click **Activation Report**.
5. On the Activation Report page, select **Show Most Recent Activations**.
6. Click **Show Results**.

It may take several minutes to process the information and make it available. Your device should show in the results grid on the Activation Report. If it doesn't show on that report, the device has failed to contact the Monitoring Center. To force a test call, see [Forcing a call to the Monitoring Center](#).
Installing the agent on multiple devices

You can deploy the Absolute agent to your computer fleet collectively—all at once or perhaps in various groups. There are several methods to install the agent on multiple devices, which are presented in this section, including:

- Deploying the agent using disk imaging
- Deploying the agent using SCCM
- Deploying the agent using Active Directory

Deploying the agent using disk imaging

Disk imaging is used to copy standard applications onto new or repurposed computers. Incorporating an unactivated agent in disk images ensures that all managed devices are protected with Absolute.

**IMPORTANT** The disk image must include an unactivated agent so each device gets a unique Identifier on the device’s first call to the Monitoring Center.

Before you begin

**To prepare a disk image:**

1. Ensure that your source computer meets the following requirements:
   - A supported operating system is installed. See [Device compatibility](#).
   - All of your organization’s preferred software are configured.
   - The computer is free of viruses.
   - The agent has never been activated on this computer.
2. Disconnect the source computer from the network.

**IMPORTANT** After you disconnect the computer from the network and start the agent install, do not connect to the network again until after the image is created.

Creating the disk image

**To create a standard disk image for your Windows devices:**

1. Install the agent on the source computer as instructed in the task [Installing the agent on an individual device](#).
2. With the source computer still disconnected from the network, create a hard disk image of the source computer following the instructions for your particular disk imaging software.
3. Test the disk image as follows:
   a. Deploy the disk image to a target device.
   b. Connect the target device to the network.
   c. Verify that the target device’s agent receives a unique Identifier as instructed in the task [Verifying the agent installation](#).
Deploying the agent using SCCM

You can use Microsoft System Center Configuration Manager (SCCM) to deploy the agent to a group of computers on a network. If your organization intends to use SCCM to deploy the agent to multiple Windows devices and you require assistance, contact Absolute Technical Support.

Deploying the agent using Active Directory

The AbsoluteAgent\[n].\[n]\-\[account_id\].msi installation file conforms to industry standards for MSI files, which enables network administrators to deploy the agent onto their devices using Active Directory. If your organization intends to use Active Directory to deploy the agent to multiple Windows devices and you require assistance, contact Absolute Technical Support.

Managing the agent

The agent installation package includes the Agent Management utility, which facilitates the management of individual agents. You can use the Agent Management utility to verify the state of the agent in an image before deploying the image to devices in your network.

After you've installed the agent successfully, use the Agent Management utility to perform the following administrative tasks:

- Starting the Agent Management utility
- Viewing agent call details
- Forcing a call to the Monitoring Center
- Configuring IP proxy settings
- Upgrading the agent on Windows devices
- Removing the agent from Windows devices

Starting the Agent Management utility

**IMPORTANT** If User Account Control is enabled, you must have Administrator credentials to manage the agent.

To start the Agent Management utility on a Windows device:

1. Using Windows Explorer, browse to the folder that contains the agent installation package that you extracted when you installed the agent previously. See Using the Agent Management utility.
2. Double-click the ctmweb.exe file to start the Agent Management utility and open the CTMWeb login page.
3. In the Please enter your password field, type password, which is the default administrative password, and then click Next.

Viewing agent call details

The Agent Status page provides the following fields:
Managing the agent

- **CTMWeb Build #**—version number of the CTMWeb application, also known as the Agent Management utility.
- **Agent Build #**—version number of the agent installed on the device.
- **Agent Mode**—state of the installed agent, showing the following possible values:
  - **Active**—the agent is installed and active.
  - **Call Support**—a problem exists with the agent. See [Contacting Absolute Technical Support](#).
- **ESN**—unique Identifier assigned to the installed agent.
- **Last IP Call Date/Time**—date and time of the last successful agent call using Internet Protocol from the device to the Monitoring Center.
- **Next IP Call Date/Time**—date and time of the next scheduled call using Internet Protocol from the agent on the device to the Monitoring Center.

**IMPORTANT** If the **Last IP Call Date/Time** field reads **No last call**, your device failed to contact the Monitoring Center. When the agent call is in progress or your device is not connected to a network, this field shows a question mark (?)

- Disregard the following fields as they were deprecated:
  - **Last Modem Call Date/Time**
  - **Next Modem Call Date/Time**

### Forcing a call to the Monitoring Center

To request that the agent contacts the Monitoring Center immediately, you can send a test call using the Agent Management utility.

→ **To force a call:**

1. Connect the device to the Internet.
2. Start the Agent Management utility. See [Starting the Agent Management utility](#).
3. Click the **Test Call** tab.
4. Click **Start** to force the call.

   The agent attempts to contact the Monitoring Center. The **Call status** field shows progress information and the screen refreshes the status automatically.

   If the call was successful, the **Call status** field shows **Passive (Last call successful)**.

   If the call failed, the **Call status** field shows **Passive (Last call failed)**. Check that the device is connected to the Internet. If so, attempt the test call again. If your next call still fails, contact [Absolute Technical Support](#).

5. To verify the success of a test call, click the **Status** tab and review the following fields on the Status page of the CTMWeb application:
   - **Last IP Call Date/Time**—shows the current date and time.
   - **Next IP Call Date/Time**—shows updated values.

### Configuring IP proxy settings

The agent can access the Internet using a proxy server to contact the Monitoring Center.
To set the account used to access a proxy server:
1. Start the Agent Management utility. See Starting the Agent Management utility.
2. Click the Options tab.
3. In the Name field, type the user name for the agent to access the Internet using a proxy server.
4. In the Password field, type the password for the agent to access the Internet using a proxy server.
5. To save your changes click Apply.
6. To confirm that the agent is functioning correctly using the new settings, make a test call to the Monitoring Center. See Forcing a call to the Monitoring Center.

Upgrading the agent on Windows devices

If your account is configured to allow automatic agent upgrades, your managed Windows devices are upgraded as new agents become available. After a new agent is released, your Windows devices are upgraded on the next agent call.

If you want to prevent automatic agent upgrades to Windows devices in your account, you can use the Agent Management area to manually update the agent to your managed devices. For more information, see Controlling Absolute agent upgrades in the online Help.

Removing the agent from Windows devices

You may want to remove the agent from a device for various reasons, such as retirement, disposal, or end of lease. Use the Unenroll Device feature in the Absolute console to remove the agent from one or more devices. For more information, see Unenrolling devices from your account in the online Help.
Chapter 3: Installing and managing the agent on Mac devices

This chapter provides information about device compatibility and instructions for installing the Absolute agent on Apple® Mac devices in the following ways:

- **Direct installation**: commonly used to install the agent on individual computers not connected through a network. This method requires hands-on contact with each target device. For details about this type of installation, see [Downloading and installing the agent on an individual device](#).
- **Batch installation**: used to install the agent on multiple devices. For details about this type of installation, see [Installing the agent on multiple devices using disk imaging](#).

This chapter also includes information about managing the agent on your Mac devices. The agent installation package includes the Agent Management utility. You can use this application to manage individual agents and to verify the state of the agent in an image before deploying the image to devices in your network.

This chapter includes the following sections:

- **Device compatibility**
- **Downloading and installing the agent on an individual device**
- **Installing the agent on multiple devices using disk imaging**
- **Managing the agent**

### Device compatibility

To ensure that your Mac devices are compatible with the agent, you need to meet the following requirements:

- Intel-powered hardware that supports one of the following Mac operating systems:
  - macOS 10.13
  - macOS 10.14
  - macOS 10.15

**NOTE** The Data Delete feature is supported on devices running macOS 10.13 or 10.14 only.

- Internet connection

### Downloading and installing the agent on an individual device

The instructions in this section apply to installing the agent on individual devices, which requires hands-on contact with each target device. This installation method is often used to install the agent on devices that are not connected to a network.

This section includes the following topics:

- **Before you begin**
- **Downloading the Installer**
• Installing the agent on an individual device
• Verifying the agent installation

Before you begin

To prepare for installing the agent on Mac devices:

• Use a virus-scanning program to ensure that your hard drive is free from viruses.
• Disable all resident virus-scanning programs.

**NOTE** Remember to enable all virus-scanning programs again after installing the agent successfully.

• Ensure the device is connected to the Internet.
• Ensure that you have Administrator privileges on the device.

Downloading the Installer

Before you can install the agent on Mac devices, you need to download the Full Agent Installer dmg file. You can use this installer to deploy the agent package from the command line or the InstallShield wizard.

**IMPORTANT** Where the version and account numbers are included in a filename, the convention used shows up to four digits <n>.<n>.<n>.<n>, which indicates a release number of up to four-digits, and then a hyphen and your customer account identifier (for example, 7.2.0.1-4757.dmg). For the purposes of illustration, this guide will show the version number using two digits.

The extracted agent installation package includes the following key components:

• The ddsinfo.tar file, which is the Agent Management utility.
• AbsoluteAgent<n>.<n>-.<account_id>.pkg file in the Mac Installer package format.
• A readme.txt file that includes the Agent release notes for the current release, in all supported languages.

⇒ To download the agent installer from the Absolute console:

1. Log in to the Absolute console as an Administrator with Manage permissions for Version Control and Perform permissions for Agent Installer.
2. On the navigation bar, click > Agent Management.
3. On the Agent Management page next to the agent version that you want to download, click and click Download Full Agent Installer.
4. On the Download Full Agent Installer dialog, do one of the following:
   a. Next to macOS click the Generate package link to generate this agent package. A confirmation message opens. In the background the system processes your request and generates an agent package for your account. This process could take a few minutes.
   b. Click Close to close the message dialog.
   c. On the Agent Management page next to the agent version you generated, click and click the Download Full Agent Installer again.
d. On the Download Full Agent Installer dialog in the macOS row, do one of the following depending on whether the agent package is generated:
   ○ If the agent package is generated, click the Download package link. The agent package is downloaded.
   ○ If the agent package generation process is not yet complete, click ✗ to close the dialog, wait a few minutes, and try again.
   ○ If the agent package failed to generate, click ✗ to close the dialog and try again or contact Absolute Technical Support.
   - If you have generated a package for this agent version before, in the macOS row click the Download package link. The zipped agent package is downloaded.

5. Depending on your browser and operating system, you may need to click through several dialogs to Save the .dmg file to a location of your choice; for example, to the root folder for command line installations.

6. From the location where you just saved the .dmg file, extract its contents to a local folder, a network drive, or to removable media such as a USB device.

Installing the agent on an individual device

You can install the agent on individual Mac devices in the following ways:

- Installing the agent at the command line
- Installing the agent using the Installer interface

Installing the agent at the command line

➤ To install the agent on a Mac device from the command line:

1. Browse to the agent Installer folder, double-click the AbsoluteAgent<n>.<n>.<n>-<account_id>.dmg file to mount it.
2. Open a Terminal window and browse to the mounted folder (for example, /Volume/AbsoluteAgent<n>.<n>-<account_id>).
3. From the Terminal window, run the following command:
   
   installer -store -pkg AbsoluteAgent<n>.<n>-<account_id>.pkg -target /

Installing the agent using the Installer interface

➤ To install the agent using the Installer interface:

1. Browse to the location of the downloaded installer folder, double-click the AbsoluteAgent<n>.<n>-<account_id>.dmg file to mount it.
2. Double-click the .pkg file to open the Installer interface.
3. Click Continue.
4. To change the location where the agent is installed:
   a. Click Change Install Location.
   b. On the Select a Destination page, select the disk where you want to install the agent.
   c. Click Continue.
5. Click Install to perform a standard installation of the agent and to open the password dialog.
6. In the Password field, enter the Administrator password for the Mac device and click Install Software. When
you see a confirmation message, the agent is installed successfully.

7. Click Close.

Verifying the agent installation

After installation, the agent contacts the Monitoring Center and receives a unique Identifier. You can verify that the agent was installed successfully on your devices in the following ways:

- Using the Agent Management utility
- Using the Absolute console

Using the Agent Management utility

You can verify that an agent is activated and calling in successfully using the Agent Management utility.

To verify the agent installation using the Monitoring Center:

1. Ensure that the device is connected to the Internet.
2. Open the Agent Management utility by doing the following:
   a. Browse to the folder that contains the agent installation package.
   b. Double-click the ddsinfo.tar file and extract it.
   c. Double-click the DDSInfo file to open the Agent Management utility.
   d. In the Password field, enter the Administrator password for the Mac device and click OK. The Agent Management utility opens.
3. To verify that the agent installed successfully, review the following fields:
   - Agent Version
   - Agent Mode—confirm that the value is Active.
   - ESN—Electronic Serial Number, which is also referred to as the unique Identifier. For activated agents, the last four characters of the Identifier are greater than 0000. If the last four characters are 0000, the device failed to contact the Monitoring Center. The Call Status shows on screen.
   - Last IP Call Time—shows the date and time of the most recent successful agent call.
     IMPORTANT If the Last IP Call Time field reads No last call, the device failed to contact the Monitoring Center. To force a test call, see Forcing a call to the Monitoring Center.
   - Next IP Call Time—the date and time of the next scheduled agent call from the device.

Using the Absolute console

You can verify that an agent is activated and calling in successfully by looking for the device on the Activation Report.

To view the devices in the Absolute console:

1. From the Mac device, log in to the Absolute console as an Administrator.
2. On the navigation bar, click to open the Reports page.
3. Click Go to the Classic Reports page at the bottom of the page.
4. Under Call History and Loss Control, click Activation Report.
Installing the agent on multiple devices using disk imaging

You can install the agent on multiple devices using disk imaging, which is used to copy standard applications onto unconfigured computers (devices). Incorporating the agent installer onto disk images helps to ensure that the agent is fully functional on all managed devices.

To ensure that the agent is fully functional on all managed devices:
1. Incorporate the agent Installer into a disk image on a single (source) computer.
2. Use a disk imaging program to create a complete image of the source computer's hard disk, including the agent Installer.
3. Copy this disk image to any number of identical computers (referred to as target devices).

Images created in this manner initially show a generic Identifier (with an ESN that ends in 0000) that is associated with your account. When deployed, each target device contacts your Monitoring Center when that device is first started and receives a unique Identifier.

Creating the disk image

To create a standard disk image on a source computer for your Mac devices:
1. Prepare the source computer as follows:
   a. Make sure that the source computer does not have an Absolute agent installed and activated on it. (An unactivated agent has an identifier with an Electronic Serial Number (ESN) that ends in 0000.)

      There is no requirement for network or Internet connectivity while you create the disk image. The source computer may be connected or disconnected.
   b. On a newly formatted computer, install the appropriate operating system and any other required or preferred software applications that you want to include in the disk image for your organization.
   c. Use a virus-scanning program to ensure that the source computer and all devices on which you want to install the agent are free from viruses.
2. Browse to the agent Installer folder and double-click the AbsoluteAgent<n>.<n>.<n>-<account_id>.dmg file to mount it.
3. Open a Terminal window and browse to the mounted folder (for example, /Volume/AbsoluteAgent<n>.<n>.<n>-<account_id>).
4. From the Terminal window, run the following command:

    installer -pkg AbsoluteAgent<n>.<n>.<n>-<account_id>.pkg -target /
    sudo launchctl unload /Library/LaunchDaemons/com.absolute.rpcnet.plist

IMPORTANT Do not restart the source computer. Do not force an agent call.
After a restart, the agent contacts the Monitoring Center to receive a unique Identifier. It is imperative that the agent is not able to secure a unique Identifier before you create the disk image.

5. Use the Agent Management utility to verify that the Identifier ends in 0000, which indicates that the agent is not activated.
6. Use the disk imaging software of your choice to create a hard disk image of the source computer.

NOTE The process of creating a disk image varies depending on your software. For more information on creating a disk image, refer to the user guide for your disk imaging software.

7. Test the new disk image as follows:
   a. Deploy the disk image to a target device.
   b. Connect the target device to the Internet, if it is disconnected.
   c. Restart the target device to initiate an agent call.
   d. Verify that the target device’s agent has received a unique Identifier as instructed in the task Downloading and installing the agent on an individual device.

Managing the agent

The agent installation package includes the Agent Management utility, which you can use to manage a device's agent. If you are deploying the agent to multiple devices, you can use the Agent Management utility to verify the state of the agent in an image before deploying the image to devices in your network. For more information, see Installing the agent on multiple devices using disk imaging.

The steps for installing and using the Agent Management utility vary depending on the version of the Mac agent you installed. This section includes the following sections:

- Managing the agent on Mac devices
- Upgrading the agent on Mac devices
- Removing the agent from Mac devices

Managing the agent on Mac devices

After you have installed the agent successfully, you can use the Agent Management utility to perform the following administrative tasks:

- Starting the Agent Management utility
- Viewing the agent's status and call details
- Forcing a call to the Monitoring Center

Starting the Agent Management utility

The agent installation package includes one file: DDSInfo. Installing the agent does not create another copy on the device.

IMPORTANT Absolute recommends that you remove the installation files from the local device after you complete the management tasks.
To start the Agent Management utility:
1. Ensure that the device is connected to the Internet.
2. Browse to the folder that contains the agent installation package.
3. Double-click the ddsinfo.tar file and extract it.
4. Double-click the DDSInfo file.
5. In the Password field, enter the Administrator password for the Mac device and click OK.

The Agent Management utility opens.

Viewing the agent's status and call details

To view the agent's status and call details:
1. Start the Agent Management utility. See Starting the Agent Management utility.
2. Review the following fields:
   - **Agent Version**—the version number of the agent installed on the device.
   - **Agent Mode**—the state of the installed agent, showing the following possible values:
     - **Active**—the agent is installed and running.
     - **Inactive**—the agent is installed but it is not running.
     - **Not installed**—the agent is not installed on the device.
     - **Disabled**—the agent is either flagged for removal or is removed.
   - **ESN**—the unique Electronic Serial Number (Identifier) assigned to the installed agent.
   - **Last IP Call Time**—the date and time of the last successful agent call from the device to the Monitoring Center.
   - **Next IP Call Time**—the date and time of the next scheduled call from the agent on the device to the Monitoring Center.
   - **Call Status**—shows one of the following possible values:
     - **Passive**—the agent is installed and awaiting instruction.
     - **Calling**—the agent is calling the Monitoring Center.
     - **Call succeeded**—the agent call to the Monitoring Center was successful.
     - **Call timed out**—the agent call was not made within the allowable time.
     - **Call failed**—the agent call to the Monitoring Center failed.
     - **Agent version is no longer supported**—a 32-bit version of the agent is installed. This version is no longer supported on the device. Download and install a 64-bit Mac agent (version 966 or higher).

Forcing a call to the Monitoring Center

This section includes the following topics:
- Forcing a call using the Agent Management utility
- Forcing a call from the command line

Forcing a call using the Agent Management utility

You can use the Agent Management utility to force a call to the Monitoring Center.
To force a call using the Agent Management utility:
1. Ensure the device is connected to the Internet.
2. Open the Agent Management utility. See Starting the Agent Management utility.
3. Click Test Call.

The agent attempts to contact the Monitoring Center. The Call status field shows progress information and the screen refreshes the status automatically.

If the call was successful, the Call status field shows Call succeeded.
If the call timed out or failed, check that the device is connected to the Internet. If it is, attempt the test call again. If your next call still fails, contact Absolute Technical Support.

4. To verify the success of a test call, review the following fields:
   - Last IP Call Time—shows the current date and time.
   - Next IP Call Time—shows updated values.

Forcing a call from the command line

To use the command line to force a call to the Monitoring Center:
1. On the Mac device open the Terminal application.
2. At the shell prompt, type the following command:
   ```bash
   ps -ax | grep -i rpc
   ```
   Press Return.
3. Find the process ID associated with `/Library/.rpcnet/rpc.net' -d.

   This is the agent call process. The presence of this process confirms that the agent was installed successfully.
4. To force the agent call process:
   a. At the shell prompt, type:
      ```bash
      sudo kill -s USR2 <PID>
      ```
      where <PID> is the process ID found in the previous step.
   b. Press Return.
   c. At the Password prompt type the password you used to log in to the device.

The process is stopped, and then it is restarted automatically, which forces an agent call.

Upgrading the agent on Mac devices

If your account is configured to allow automatic agent upgrades, your managed Mac devices are automatically upgraded as new agents become available. After a new agent is released, your Mac devices are upgraded on the next agent call.

If your account is not configured to allow automatic agent upgrades, as per an alternate Service Agreement, contact Absolute Technical Support to request an upgrade to the latest version of the agent for Mac.
Removing the agent from Mac devices

You may want to remove the agent from a device for various reasons, such as retirement, disposal, or end-of-life/end-of-lease. You can use the Unenroll Device feature in the Absolute console to remove the agent from one or more devices. For more information, see the online Help.
Chapter 4: Installing and managing the agent on Android devices

This chapter provides instructions for installing and managing the Absolute agent on devices that run on the Android™ operating system.

This chapter includes the following sections:

- Device compatibility
- Downloading and installing the Absolute Agent for Android
- Managing the agent using the Absolute Dashboard
- Upgrading the agent
- Removing the agent

Device compatibility

The agent supports all makes and models of devices running Android versions 4.2.2 to 10.0.

**NOTE** If you are installing the Absolute agent on an Android 10 device, ensure that you install agent version 3301 or higher.

Downloading and installing the Absolute Agent for Android

The instructions in this section apply to installing the agent on individual Android devices, which requires hands-on contact with each target device.

This section contains the following topics:

- Before you begin
- Downloading the Absolute Agent for Android Installer
- Installing the Absolute Agent for Android on your devices

Before you begin

The agent is not available from the Google Play Store. You need to download it directly to the device before you can install it. By default, Android devices do not allow installation of applications from unknown sources. Therefore, you need to change the settings on your device before installing the agent.

→ To allow for the installation of unknown sources:

1. Log in to the mobile device.

**NOTE** If the device supports multiple users, ensure that you are logged in as the Owner (primary user).
2. Open the **Settings** menu of your device and tap **Security**.
3. Select the **Unknown sources** checkbox.
4. If a warning message opens, tap **OK**.

You can now install applications from a source other than Google Play Store on your Android device.

### Downloading the Absolute Agent for Android Installer

The Absolute Agent for Android Installer, which is distributed as the **CTMobile.apk** file, contains the following components depending on the version of the package you downloaded:

- **Absolute Sentinel** (on selected devices only)—the Absolute Sentinel application, which ensures that the Absolute Agent for Android is running at all times.
- **Absolute Mobile Agent** (mandatory)—the Absolute Agent for Android.
- **Absolute Dashboard** (optional)—the Absolute Dashboard application, where you perform functions such as:
  - viewing the status of the agent
  - forcing a test call
  - generating a log file for troubleshooting purposes

➤ **To download the Absolute Agent for Android Installer:**

1. Using your computer, log in to the Absolute console as an Administrator.
2. On the navigation bar, click 📥.
3. On the Settings sidebar, click **Download Packages**.
4. On the Download Packages page in the **Agent Type** column of the **Agent** table, click the **Android** link and download the file.

**NOTE**  Depending on your browser, you may need to confirm the download by clicking the information bar and clicking the **Android** link again.

5. Navigate to the **.htm** file that you downloaded in the previous step and open it.
6. To send the download link to the Android device, select one of the following options:
   - To install the Absolute Agent for Android without the Absolute Dashboard:
     a. In the **Agent Only** field click **Send URL by Email**, which opens a new email message using your default email program.
     b. Enter the appropriate email address and send the message.
   - To install the Absolute Agent for Android and the Absolute Dashboard:
     a. In the **Agent with Dashboard** field click **Send URL by Email**, which opens a new email message using your default email program.
     b. Enter the appropriate email address and send the message.

**NOTE**  If you do not want to distribute the download links that contain the product key information, you can send the link using one of the **Send URL by Email** links in the **Alternative method** section. Using the **Alternative method** includes the **Install Key** and the **Pass Phrase** in the body of a new email.

7. Log in to the mobile device. If the device supports multiple users, ensure that you are logged in as the **Owner** (primary user).
8. Open the email that you sent to the device.
9. Tap the link provided in the email, tap **Download**, and, if a warning message shows, then tap **OK**.
NOTE If the download does not start automatically, tap the link at the bottom of the page to force the download.

You are now ready to install the Absolute Agent for Android on your device.

Installing the Absolute Agent for Android on your devices

➔ To install the agent on your devices:
1. Log in to the mobile device.

   NOTE If a device supports multiple users, ensure that you are logged in to the device as the Owner (primary user).

2. On the Launcher pane, tap the Downloads icon.
3. Tap CTMobile.apk and tap Install to start installing the Absolute Agent for Android Installer. When the installation is complete, a confirmation page opens.
4. Tap Open to open the installer.
   A list of actions that the Installer performs opens, which includes:
   - Install Sentinel (on select devices only)
   - Install Agent
   - Activate device administrator (on select devices only)
   - Activate overlays permission (on select devices only)
   - Grant default SMS for IDs and revoke later (on select devices only)
   - Grant permissions
   - Install Dashboard (if the installation package includes the Absolute Dashboard)
   - Uninstall Installer
5. Tap Install apps to start the installation process.
6. If the installation components install automatically without any further action, skip this step. Otherwise, do the following:
   a. Tap Install to start installing the Absolute Sentinel (wd.ctm) application.
      When the installation is complete, a confirmation dialog opens.
   b. Tap Done.
   c. Tap Install to start installing the agent (sec.abt).
      When the installation is complete, a confirmation dialog opens.
   d. Tap Done. A dialog opens prompting you to activate the agent.
   e. Do one of the following:
      - If you are installing the agent on a device running Android 4.4.2 to 9, tap Activate or Activate this device admin app.
      - If you are installing the agent on an Android 10 device, do the following:
        i. Tap Activate this device admin app.
        ii. On the Display over other app dialog, tap the switch to allow the agent to display over other apps.
        iii. If the default SMS app dialog shows, select sec.abt and tap Set as default.
NOTE This dialog shows if the agent is unable to detect the device's serial number, which is required to activate the agent. After the agent is activated, you'll be prompted to revert the default SMS app back to its original setting.

If you click Cancel on this dialog, the installation process is stopped because the agent can't be activated if it isn't granted default SMS app permissions. On the Install incomplete dialog that shows, click OK and then click Uninstall apps to uninstall Absolute Sentinel, the Absolute Agent, and the installer.

i. If the device location access dialog shows, tap Allow all the time.

ii. After the agent is activated, the default SMS app dialog shows again if you set sec.abt as the default. Select the original default app and tap Set as default.

f. In the series of five dialogs that show, click Allow in each dialog. The agent needs access to each of the listed phone features for it to function correctly.

g. If your installer includes the Absolute Dashboard, tap Install to install it now.

When the installation is complete, a confirmation dialog opens.

h. Tap Done.

When the installation is complete, a confirmation dialog opens indicating that you can now uninstall the Absolute Installer.

7. Tap OK.

8. Tap OK or Uninstall to uninstall the installer.

A confirmation page opens when the uninstall process is complete.

The applications are now installed on your device. If you installed the Absolute Dashboard application, the Absolute Dashboard icon shows on the Launcher pane of your device.

For more information, see Managing the agent using the Absolute Dashboard.

IMPORTANT If the version of the Absolute Agent for Android Installer you downloaded does not include the Absolute Dashboard, you do not see an icon on your Launcher pane. If you want to install the Dashboard, you need to download the appropriate version of the installer and follow the installation process again.

Managing the agent using the Absolute Dashboard

The Absolute Dashboard is intended to provide diagnostic information to Administrators who manage their organization's mobile devices using Absolute for Android.

IMPORTANT To use the Absolute Dashboard application, it must be included in the version of the Absolute Agent for Android Installer you downloaded from the Absolute console.

The Absolute Dashboard application lets you perform the following tasks:

- Setting your password on first use
- Changing your password
- Viewing agent status information
- Viewing the Device State service
• Viewing the agent Logs
• Forcing a test call to the Monitoring Center
• Sending diagnostic information to Absolute Technical Support

Setting your password on first use

The first time you start the Absolute Dashboard, you are prompted to choose a password.

➤ To set your password the first time you log in to Absolute Dashboard:
  1. On the Launcher pane, tap the A icon.
  2. In the Choose a new password field, enter a new password that is at least eight characters in length. Your password can include alpha-numeric and/or special characters, including spaces.
  3. In the Confirm new password field, enter the password you entered in the previous step again.
  4. Tap Set Password to save the new password and open the Absolute Dashboard page, which shows the content of the Summary tab.

Changing your password

➤ To change your password:
  1. On the Launcher pane, tap the A icon.
  2. Enter your password and tap OK to open the Absolute Dashboard page with the Summary tab's contents showing.
  3. On the Summary page in the upper right corner is the Menu icon, which is three white circles arranged vertically. Tap the  icon and then tap Change Password.
  4. To change your password, complete each of the password fields.
  5. Tap Update Password.

Viewing agent status information

➤ To view agent status information:
  1. On the Launcher pane, tap the A icon.
  2. Enter your password and tap OK.
  3. On the Absolute Dashboard page, three tabs are available: Summary, Services, and Logs.

The Summary tab is active and provides the following information about the agent:

• Agent status—the status of the Android agent installed on the device.
  ◦ Idle—the agent is awaiting the next scheduled call.
  ◦ Not Set—the agent is not running currently.
  ◦ Activating—the agent is activating itself during this initial agent call to the Monitoring Center.
  ◦ Initiating Session—the agent is initiating a call to the Monitoring Center. This status shows at the start of every call.
  ◦ In Call—the agent is calling in currently.
  ◦ Getting Commands—the agent is receiving a list of commands to process one of the Data and Device Security features. You may see many different instances of the status because there is one for each feature that is processed.
- **Processing Command**—the agent is processing a command within a feature; for example, processing a Data Delete command to delete files and folders on the device.
- **Ending Session**—the agent is terminating the current call to the Monitoring Center.
- **Set for Removal**—the agent is flagged for removal.

- **Agent version**—the version number of the agent that is installed on the device.
- **Identifier**—the unique identifying number for this device.
- **Next call time**—the time and date of the next scheduled call from the agent on this device.
- **Last call time**—the time and date of the last scheduled call from the agent on this device.
- **Last call status**—the status of the last call to the Monitoring Center from the following possible values:
  - **Completed successfully**—the last call made to the Monitoring Center completed successfully.
  - **Activation error**—an error occurred when the agent was activating itself with the Monitoring Center.
  - **Authentication error**—an error occurred when the agent was in the Initiating Session state during the last call.
  - **Session expired or invalid**—the agent is starting a call to the Monitoring Center while another call is still active.
  - **Service error**—a general communication failure occurred.
  - **Call failed**—a general failure occurred.
- **Monitoring Center**—the URL of the server with which the agent makes a secure connection to send device authentication and inventory data, and receive various service instructions.
- **Location tracking**—indicates whether Geolocation tracking is enabled and the number of location samples collected since the last agent call.

## Viewing the Device State service

The Device State service checks periodically for new and existing policies that were configured for the device.

**To view the Device State service information:**

1. On the Launcher pane, tap the ![device](image) icon.
2. Enter your password and tap **OK**.
3. On the Absolute Dashboard page tap the **Services** tab for the status of the agent component that enables services such as Absolute Policies.

**NOTE**  
Software policy and Geolocation policy are optional. Therefore, if there is no policy set up for the device, these policies are shown as disabled.

- **Device State service**—The device periodically checks which policies are configured for the device.
  - The **Next check** indicates the next time and date that the device is scheduled to check the Device State service.
  - The **Last check** indicates the status of the last check of the Device State service and includes the following values:
    - **Successful** means the last check of the Device State service was successful.
    - **Not set** indicates the device has not called the Device State service yet.
    - **Failed** – `<error code>` indicates that the last communication with the Device State service was unsuccessful and provides the resulting error code; for example, 404, 503, and so forth.
- **Hardware scan**—indicates whether or not a hardware policy was set up for the device.
  - The **Next scan** indicates the time and date when the agent runs a hardware scan and uploads the data to the Monitoring Center.
  - The **Last upload** indicates the status of the last upload of the hardware scan to the Monitoring Center, which includes the following values:
    - **Successful** means the last upload of hardware data for the device was successful.
    - **Not set** is the initial state that indicates that no hardware data was uploaded to the Monitoring Center yet.
    - **Failed** – `<error code>` indicates that the last hardware upload was unsuccessful and provides the resulting error code; for example, 404, 503, and so forth.

- **Software scan**—indicates whether or not a software policy was set up for this device.
  - The **Next scan** indicates the time and date when the agent runs a software scan and uploads the data to the Monitoring Center.
  - The **Last upload** indicates the status of the last upload of the software scan to the Monitoring Center, which includes the following values:
    - **Successful** means the last upload of software data for the device was successful.
    - **Not set** is the initial state that indicates that no software data was uploaded to the Monitoring Center yet.
    - **Failed** – `<error code>` indicates that the last software upload was unsuccessful and provides the resulting error code; for example, 404, 503, and so forth.

- **Geolocation scan**—indicates there is a Geolocation policy applied to the device. WiFi and/or Global Positioning System (GPS) may be enabled in the policy.

There is only one upload of Geolocation scan data because the WiFi and Geolocation samples are grouped together and uploaded as a bundle. Possible values include:
  - **Next upload** indicates the time and date when the agent uploads the geolocation samples to the Monitoring Center.
  - **Last upload** indicates the status of the last upload of geolocation data to the Monitoring Center, which includes the following possible values:
    - **Successful** means the last upload of geolocation data for the device was successful.
    - **Not set** is the initial state that indicates that no geolocation data was uploaded to the Monitoring Center yet.
    - **Failed** – `<error code>` indicates that the last upload of geolocation samples was unsuccessful and provides the result error code; for example, 404, 503, and so forth.
  - **WiFi - next scan** indicates the time and date when the agent runs a WiFi geolocation scan.
  - **WiFi - samples to upload: <n>** indicates the number of WiFi samples to upload to the Monitoring Center on the next upload.
  - **GPS - next scan** indicates the time and date when the agent runs a GPS geolocation scan.
  - **GPS - samples to upload: <n>** indicates the number of GPS samples to upload to the Monitoring Center on the next upload.

**Viewing the agent Logs**

On the Absolute Dashboard, the **Logs** tab provides a list of errors, if any, that the Absolute agent encountered during the last call to the Monitoring Center. If the Geolocation tracking feature reports any errors outside of an agent call, these errors are also available in the agent Logs.
To view the agent Logs:
1. On the Launcher pane, tap the icon.
2. Enter your password and tap OK.
3. On the Absolute Dashboard page, tap the Logs tab.
4. To view updated agent call information on the Logs page, tap the icon and tap Refresh.

Forcing a test call to the Monitoring Center

To force a test call:
1. On the Launcher pane, tap the icon.
2. Enter your password and tap OK.
3. On the Absolute Dashboard page with the contents of the Summary page showing, tap Call in.

If your Android device is connected to the Internet using Wi-Fi or a data connection, the device calls the Monitoring Center.

Sending diagnostic information to Absolute Technical Support

If you experience problems with the Absolute Agent for Android, you can use the Absolute Dashboard to send Absolute Technical Support a log file that contains detailed diagnostic information about these problems.

To send diagnostic information:
1. On the Launcher pane, tap the icon.
2. Enter your password and tap OK.
3. On the Absolute Dashboard page, tap the Logs tab.
4. On the Log page, tap the icon and tap Refresh.
5. Tap the icon and tap Send log.
6. If the device is running the Android 6.0 (Marshmallow) operating system, a message shows indicating that you need to grant Storage permissions. If Absolute's Persistence technology is embedded on the device, you also need to grant Phone permissions.

To proceed:
   a. In the message dialog, tap OK.
   b. In each dialog that shows, tap Allow. If you do not grant Storage permissions, the log file is not sent. If you do not grant Phone permissions, the log file is sent, but it does not include any mobile device identifiers, such as the IMEI.
7. Depending on how many mailboxes you have set up on your device, one of the following happens:
   a. If you have only one email program set up on your device, the Compose email window opens. Proceed to the next step.
   b. If you have set up more than one email program on your device, the Choose email application dialog opens. Tap the appropriate application name. If possible, we recommend that you use Gmail.

   The Compose email window opens.
8. By default, the agent log is sent to SupportLogFile@absolute.com.
   a. To send the agent log to another email recipient, in the To field enter the new email address.
   b. To add other email recipients, in the To field enter each email address, separated by commas.
9. Tap Done.

The email and the attached agent log are sent to the specified recipients.

**Upgrading the agent**

When your account is configured to allow automatic agent upgrades, your managed Android devices are upgraded automatically as new agents become available. After a new agent is released, your Android devices are upgraded on the next agent call.

If your account is not configured to allow automatic agent upgrades, as per an alternate Service Agreement, contact Absolute Technical Support to request an upgrade to the latest version of the Absolute Agent for Android.

**Removing the agent**

You may want to remove the Absolute Agent for Android from a device for various reasons, such as retirement, disposal, or end-of-lease. You can use the Unenroll Device feature in the Absolute console to remove the agent from one or more devices. For more information, see the online Help.
Chapter 5: Deploying and managing the Chromebook extension

This chapter describes how to deploy the Absolute for Chromebooks extension (Chromebook extension) to your Chromebooks, manage your Google account in Absolute, and unenroll devices from Absolute.

NOTE This chapter only applies to customers with a license that includes Chromebook support.

You can see either the Chromebooks - Google Account area at the bottom of the > Classic Account Settings page, or > Chromebook settings. Where indicated, follow the instructions associated with the setting that you see. If you see the Chromebooks - Google Account area, use the Classic instructions. If you see > Chromebook settings, use the Absolute 7 instructions.

This chapter includes the following sections:

- Device compatibility
- Configuring and deploying the Chromebook extension
- Managing your Google account details in the Absolute console
- Removing the Chromebook extension

Device compatibility

To support the Chromebook extension, devices must be running Chrome OS version 73 or higher. Devices must also be managed in the Google Admin Console.

Configuring and deploying the Chromebook extension

The instructions in this section are for deploying the Chromebook extension on devices, which doesn't require hands-on contact with each target device. To use the Chromebook extension, add your Google account to the Absolute console and make changes to the settings in the Google Admin console. If you are licensed for Investigations support, configure a "Stolen" organizational unit (OU).

IMPORTANT To ensure the proper deployment of the Chromebook extension, you must complete all three of the following tasks:

- Adding your Google account to Absolute
- Configuring settings in the Google Admin Console
- Deploying the Chromebook extension to users

You only need to complete Configuring the Stolen OU if you are licensed for Investigations support.

Before you begin

Before you begin the tasks described in this section, make sure that:
You are assigned a Google Admin role with the following minimum set of administrator privileges:

- **Organizational Units**, including Create, Read, Update, and Delete privileges
- **Users**, including Read privileges
- **Services > Chrome management**, including Manage Devices, 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.

You have added at least one OU under your domain in your Google account and the Chromebook devices you want to add to the Absolute console are contained in it

For more information about creating Google OUs, see Google Admin Console documentation.

**NOTE**  If you have not purchased enough licenses for all the Chromebooks in your fleet, ensure that the Chromebooks you want to add to the Absolute console are in their own OUs directly under your organization. By doing so, you ensure that only available licenses are consumed.

API access in enabled for your Google account (Absolute 7 only)

To simplify the configuration of OUs in the Google Admin Console, you can create a parent OU that contains all the OUs with devices you want to sync to the Absolute console and all the OUs with users that you want to deploy the Chromebook extension to. Child OUs inherit the settings from the parent OU by default. You can deselect child OUs in the Absolute console if you don’t want to sync the devices in it to your Absolute account.

For more information about creating Google OUs, see Google Admin console documentation.

**Adding your Google account to Absolute**

To add your Chromebooks to your Absolute account, you need to add your Google account name in the Absolute console and select the OUs that you want to sync. This allows Absolute to retrieve the data used to activate the Chromebook extension and supplement data reported by the Chromebook extension.

Use either the instructions for Classic or Absolute 7 depending on the setting that you see in the Absolute console:

- **To add your Google account name - Classic**
- **To add your Google account - Absolute 7**

**To add your Google account name to your Absolute account - Classic:**

1. Log in to the Absolute console as an Administrator.
2. On the navigation bar, click > 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.
   
   You are redirected to Google’s authentication page. Follow the prompts provided by Google to sign in to your account and allow Absolute access.
5. In the Select Organizational Units dialog, select each OU containing the Chromebooks you want to add to your Absolute account.
Note: Google restricts the OAuth 2.0 scopes that Absolute must request to access your Google account information using the Google APIs. These scopes are the minimum required to sync Google data into Absolute.

Your Google account and its OUs show in the work area on the Chromebook Settings page.

5. After returning to the Absolute console, select the check box next to each OU containing the Chromebooks you want to sync. Selecting a parent OU selects the children of the parent. To remove a selection, clear its check box.

   Use one of the following methods to find the OUs you want to sync:
   - To search for an OU, type all or part of the OU name in the Search Organizational Units field. The search results update dynamically as you type. If the OU is a sub organization it shows in the search results as a child of its parent.
   - To navigate the organizational structure to find the OU, scroll the page to find the item. You can click the icon to expand an item and see its sub organizations.

   After two seconds, your changes are automatically saved.

   Absolute schedules a sync with your Google account in 20 minutes time. The sync should take no longer than an hour. When this process is complete, the date and time are populated below the Google account in the sidebar in the Chromebook Settings page. After the initial sync, Absolute schedules an automatic sync every 24 hours.

Go to Configuring settings in the Google Admin Console to complete the next step in the configuration.

Configuring settings in the Google Admin Console

To ensure that your Chromebook devices fully support the Chromebook extension, you must configure both Device settings and User & browser settings in the Google Admin Console. There are additional settings that only need to be
updated if they are no longer set to their default values. Occasionally, review all your Chromebook settings to ensure they haven't been changed accidentally.

**Editing Device settings**

**NOTE** If all of your devices are in OUs under a parent OU, complete the following steps once with the parent OU selected. If they are not under a parent OU, make sure you complete these steps for each OU that contains Chromebook devices that you want to synchronize with the Absolute console.

→ **To edit Device settings:**

1. Log in to the Google Admin console using the credentials for the account that you use to manage your devices.
2. From the Google Admin console home page, navigate to Devices > Chrome management > Device settings.
3. Select the OU containing the Chromebook devices you want to add to Absolute and edit its Device settings as follows:
   a. In the Enrollment and access section, set the **Forced re-enrollment** field to **Force device to automatically re-enroll into this domain after wiping**.
   b. In the Sign-in settings section:
      i. set the **Guest mode** field to **Disable guest mode**.
      ii. set the **Sign-in restriction** field to **Restrict sign-in to a list of users** and enter *@<YourDomain.com>* in **User whitelist**.
4. Click **SAVE**.

**Reviewing Device settings**

If you haven't changed the default values for the following settings, no action is required. If you are unsure, you can verify these settings and update them if they differ.

- In the Device settings section:
  - the **Auto-update settings > Automatic updates** field should be set to **Allow auto updates**, which enables updates to the Chromebook extension to be deployed automatically to the device.
  - the **Release channel** field should be set to **Stable**.
- In the Kiosk settings section, set **Managed guest session** to **Do not allow managed guest sessions**.

**Editing User & browser settings**

**NOTE** If all of your users are in OUs under a parent OU, complete the following steps once with the parent OU selected. If they are not under a parent OU, make sure you complete these steps for each OU containing users you want to deploy the Chromebook extension to.

→ **To edit User & browser settings:**

1. Log in to the Google Admin Console using the credentials that you use to manage your users.
2. From the Google Admin console home page, navigate to Devices > Chrome management > User & browser settings.
3. Select the OU containing the users you want to deploy the Chromebook extension to and edit its User &
Browser settings as follows:

a. In the Security section, set the Geolocation field to Allow sites to detect users' geolocation.

   NOTE If the Geolocation field is set to Do not allow sites to detect users' geolocation, no location data is sent to Absolute.
   If the Geolocation field is set to Allow the user to decide or to Always ask the user if a site wants to detect their geolocation, and the user turns off geolocation, no location data is sent to Absolute.

b. In the User experience section, set the Developer tools field to either Allow use of built-in developer tools except for force-installed extensions or Never allow use of built-in developer tools.

c. Click SAVE.

d. Scroll up to the Apps and extensions section and click application settings page.

e. In the Additional applications settings section, select all the apps and extensions in Allowed types of apps and extensions.

f. Click SAVE.

Reviewing User & browser settings

If you haven't changed the defaults for the following settings, no action is required. If you are unsure, you can verify these settings and update them if they differ.

- In the General section, the Smart Lock for Chrome field should be set to Do not allow Smart Lock for Chrome.
- In the Enrollment controls section:
  - the Device enrollment field should be set to Keep Chrome device in current location.
  - the Enrollment permissions field should be set to Allow users in this organization to enroll new or re-enroll existing devices.

Go to Deploying the Chromebook extension to users to complete the next step in the configuration.

Deploying the Chromebook extension to users

Absolute distributes the Chromebook extension through the Chrome Web Store. This section describes how to use the Extension ID to find the extension and configure it as a force-installed app in the Google Admin Console. The extension only loads and operates properly on Chromebooks that are active in the Absolute console.

NOTE If all of your users are in OUs under a parent OU, complete the following steps once with the parent OU selected. If they are not under a parent OU, make sure you complete these steps for each OU containing users you want to deploy the Chromebook extension to.

⇒ To deploy the Chromebook extension:

1. Log in to the Absolute console as an Administrator.
2. On the navigation bar, click Download Packages.
3. On the Download Packages page, scroll to the Absolute for Chromebooks Extension section.
   - In the Extension ID column of the table, click the Copy to Clipboard link. The extension ID is copied to your clipboard.
4. Log in to the Google Admin console using the credentials for the account that you use to manage your users.
5. From the Google Admin console home page, navigate to Devices > Chrome management > User & browser settings.
6. Select the OU that contains the users you want to deploy the Chromebook extension to.
7. Scroll to the Apps and extensions section and click apps & extension page.
8. Hover over + and click 📎Add Chrome app or extension by ID.

   Paste the Extension ID you copied from the Absolute console into the Extension ID field, and click SAVE.
10. Click SAVE.

The Chromebook extension is saved to the list of force-installed apps for your device. When an authorized user logs in to the Chromebook, the extension is deployed to the device.

After the extension is deployed to your Chromebook devices, it is activated with its first secure connection to the Absolute Monitoring Center. The extension then makes regularly scheduled connections to the Monitoring Center on a daily basis. During these connections, the extension sends the latest device data to the Monitoring Center and instructions for any pending security operations, such as Device Freeze, are sent to the device. Data from the Chromebook extension is periodically synchronized into Absolute reports.

If your license includes the Investigations feature, go Configuring the Stolen OU to complete the final step in the configuration.

If your license doesn't include the Investigations feature, you have successfully deployed the Chromebook extension.

**Configuring the Stolen OU**

**NOTE** This task is only required if your license includes the Investigation feature.

If you are licensed for Investigations support, you need to configure a "Stolen" OU to help the Investigations team track and recover Chromebooks that your organization has reported stolen. After creating the Stolen OU, associate a Managed guest session with the OU and configure Device settings for the OU.

If you haven't set up a Stolen OU, complete the following tasks:

- Creating the Stolen OU
- Configuring the Stolen OU

If you have previously set up the Stolen OU with the Kiosk app, change the Stolen OU to use a Managed guest session. To switch to a Managed guest session, you need to complete both the following tasks:

- Deleting the Kiosk app
- Configuring the Stolen OU

For more information about the Managed guest session, see What effect does a Managed guest session have on a stolen Chromebook?
Creating the Stolen OU

➤ To create the Stolen OU:

1. Log in to the Google Admin console using the credentials for the account that you use to manage your devices.
2. Under your domain in your Google account, create an OU and name it Stolen. Ensure that you create the OU at the root of your domain. The Stolen OU needs to be in place before the Absolute Investigations team can track and recover a Chromebook if it is stolen.

IMPORTANT You must name the OU Stolen with no variation. If you don't use the exact name, the Investigations team can't track and recover a stolen Chromebook.

To finish setting up the Stolen OU, complete Configuring the Stolen OU.

Deleting the Kiosk app

Only complete this step if you have previously set up the Stolen OU to use the Kiosk app.

➤ To delete the Kiosk app:

1. Log in to the Google Admin console using the credentials for the account that you use to manage your devices.
2. Select the Stolen OU.
3. From the Google Admin console home page, navigate to Devices > Chrome management > Device settings.
4. In the Kiosk settings section, click apps & extensions page.
5. Click the Browser app and click 📋.
6. Click SAVE.

To configure a Managed guest session, complete Configuring the Stolen OU.

Configuring the Stolen OU

➤ To configure the Stolen OU

1. Log in to the Absolute console as an Administrator.
2. On the navigation bar, click 🗂 > Download Packages.
3. On the Download Packages page, scroll to the Absolute for Chromebooks Extension section.
   In the Extension ID column of the table, click the Copy to Clipboard link. The extension ID is copied to your clipboard.
4. Log in to the Google Admin console using the credentials for the account that you use to manage your devices.
5. From the Google Admin console home page, navigate to Devices > Chrome management > Managed guest session settings.
6. Select the Stolen OU and edit its Managed guest session settings as follows:
a. In the General section:
   i. set the Managed guest session field to Auto-launch managed guest session.
   ii. enter the name you want your users to see for the Managed guest session in Session name to display on the login screen. For example, "Guest mode" or "School Name Chromebook".

b. In the Security section, set the Incognito mode field to Disallow incognito mode.

7. Click SAVE.
8. In the Apps and extensions section, click apps & extensions page.
9. With the MANAGE GUEST SESSIONS tab selected, hover over + and click Add Chrome app or extension by ID.
   Paste the Extension ID you copied from the Absolute console into the Extension ID field, and click SAVE.

10. Next to the Absolute for Chromebooks app, select Force install from the Installation policy drop-down.
11. Click SAVE.

   The Chromebook extension is saved to the list of force-installed apps for your device for the Stolen OU.

12. From the Google Admin console home page, navigate to Devices > Chrome management > Device settings.
13. Edit the Device settings as follows:
   a. In the Enrollment and access section, set the Forced re-enrollment field to Force device to automatically re-enroll into this domain after wiping.
   b. In the Sign-in settings section:
      i. set the Guest mode field to Disable guest mode.
      ii. set the Sign-in restriction field to Restrict sign-in to a list of users and enter *@<YourDomain.com> in the User whitelist field.
   c. In the Kiosk settings section, set Managed guest session to Auto-launch managed guest sessions.
   d. In the User and device reporting section, set both Device reporting fields to Enable device state reporting and Enable tracking recent device users.

14. Click SAVE.
15. From the Google Admin console home page, navigate to Devices > Chrome management > User & browser settings.
16. In the Security section, set the Geolocation field to Allow sites to detect users' location.
17. Click SAVE.

In the future, when you report a Chromebook stolen, the Absolute Investigations Team moves the device to the Stolen OU, which forces the device to open in a Managed guest session. Depending on the polling time period set for your Google account, it may take up to 24 hours for the Chromebook to open in a Managed guest session. If the device is restarted, it opens in a Managed guest session immediately. Using a Managed guest session helps the Investigations Team track and recover the Chromebook.

**What effect does a Managed guest session have on a stolen Chromebook?**

After the Managed guest session is running on the Chromebook, device and geolocation information is sent to the Absolute Monitoring Center where it is made available to the Absolute Investigations Team to assist in the device’s recovery.

From a user’s perspective, stolen devices in a Managed guest session have the following characteristics:
• The user sees a message that their activity is being monitored when the device is restarted.
• The user is automatically logged in to guest mode when they reach the Chrome OS login screen.
• The user can configure settings local to their session.
• The user cannot add a new users.

When the device is recovered and the Absolute Investigations team closes the Investigation Report:

• The device is moved back to its original OU in your Google account.
• The device is no longer run as a Managed guest session.
• Full Chrome device functionality is restored.
Managing your Google account details in the Absolute console

This section provides information on the following topics:

- Editing Google account details
- Deleting a Google account

Editing Google account details

You can add or remove Chromebooks from your Absolute account by changing the OUs you have selected in the Absolute console.

Use either the instructions for Classic or Absolute 7 depending on the setting that you see in the Absolute console.

- To edit your Google account details – Classic
- To edit your Google account details – Absolute 7

To edit your Google account details – Classic:

1. Log in to the Absolute console as an Administrator.
2. On the navigation bar, click > Classic Account Settings.
3. Scroll to the Chromebooks - Google Account area, locate the Google account that you want to edit and click its Edit link.
4. In the Select Organizational Units dialog, select each OU that contains the Chromebooks you want to add to your Absolute account. To remove Chromebooks from your account, clear each checkbox next to the applicable OUs.
5. If you cleared any checkboxes, a warning message shows. Click Yes to continue.

WARNING Clearing the checkbox of a previously selected OU automatically sets its Chromebooks to Disabled, which frees up device licenses.

6. Click Continue to save your changes and close the dialog.

Absolute begins to update 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 in the Chromebooks - Google Account section of the Classic Account Settings page.

To edit your Google account details – Absolute 7:

To edit your Google account details:

1. Log in to the Absolute console as a user with Manage permissions for Policies.
2. On the navigation bar, click > Chromebook Settings.
3. On the sidebar, select the Google account you want to edit.
4. In the work area, select each OU that contains Chromebooks you want to add to your Absolute account. To remove Chromebooks from your account, clear each check box next to the applicable OUs.

WARNING Clearing the check box of a previously selected OU automatically unenrolls the Chromebooks that belong to the OU and sets their Agent Status to Disabled, which frees up device licenses.
After two seconds, your changes are automatically saved.

Absolute schedules a sync with your Google account in 20 minutes time. The sync should take no longer than an hour. When this process is complete, the date and time are populated below the Google account in the sidebar in the Chromebook Settings page.

**IMPORTANT**  Adding Chromebook devices to your account is a two step process. If the new OUs are children of a parent OU that you have already changed the Device settings for, you are done. If they are not, make sure you also update the Device settings. See Configuring settings in the Google Admin Console.

### Deleting a Google account

If a Google account was added in error, or the account is not required anymore, you can delete it from the Absolute console.

Use either the instructions for Classic or Absolute 7 depending on the setting that you see in the Absolute console.

- [To delete a Google account - Classic](#)
- [To delete a Google account - Absolute 7](#)

**To delete a Google account – Classic:**

**WARNING**

Use caution when deleting an existing Google account from the Absolute console. 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](#).

1. Log in to the Absolute console as an Administrator.
2. On the navigation bar, click > Classic Account Settings.
3. Scroll to the Chromebooks - Google Account area, locate the Google account that you want to delete and click its Delete link.
4. On the confirmation message, click OK.

Absolute begins to update 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 in the Chromebooks - Google Account section of the Classic Account Settings page.

**To delete a Google account – Absolute 7:**

**WARNING**

Use caution when deleting an existing Google account from the Absolute console. This action has the following effect on Chromebooks in the Absolute console:
• The Agent Status is changed to Disabled. The devices can still be viewed in reports by settings the report’s Agent Status filter to Disabled.
• Device information is no longer synchronized between your Google account and your Absolute account. Any existing data showing in Absolute reports remains available, but it is no longer updated.
• If you add new devices to your Google account, the devices are not added to your Absolute account.

1. On the navigation pane, click > Chromebook Settings.
2. On the sidebar, select the applicable Google account. The account’s OUs show in the work area with the synced OUs selected.
3. Click Remove Account and click OK.

The Google account is removed from the sidebar.

Unenrolling Chromebooks

Unenrolling a Chromebook device from your Absolute account sets the device’s status to Disabled and frees up Absolute licenses. All synchronized data remains in the database and you can still view the unenrolled device in reports by setting the Agent Status filter to Disabled.

Unenrolling Chromebooks from the Absolute console doesn't remove the Chromebook extension from users. You don't have to remove the Chromebook extension. When a user with the Chromebook extension logs in to an unenrolled device, the Chromebook pings Absolute to check to see if the device has been re-enrolled, but all other features are disabled.

If a user without the Chromebook extension associated with their OU logs into a device that is synced with Absolute, the device doesn't call in to Absolute. Unless a user with the Chromebook extension logs into the device, the device appears as a dark device in the Absolute console.

To unenroll the device, complete one of the following tasks:

• [Deprovisioning Chromebooks](#)
• [Moving the device to an unsynced OU](#)
• [Deselecting the device’s OU](#)
• [Using the Unenroll Device action](#)

Deprovisioning Chromebooks

When you deprovision the Chromebook device in the Google Admin Console, Absolute retrieves the device's Deprovisioned status during the next sync of the device and sets the device's Agent Status to Disabled.

For more information about deprovisioning Chromebook devices, see Google Admin Console documentation.

Moving the device to an unsynced OU

An unsynced OU is an OU that isn't selected in > Chromebook settings in the Absolute console.
To move the device to an unsynced OU:

1. Log in to the Google Admin console using the credentials for the account that you use to manage your devices.
2. From the Google Admin console home page, navigate to Devices > Chrome management > Devices.
3. On the navigation pane, search for and select the OU that contains the devices you want to unenroll.
4. In the Devices list, select the checkbox next to each device.
5. In the taskbar, click Move selected devices.
6. In the dialog that opens, select the unsynced OU you want to move the devices to and click Move.

The next time the device calls in, the Device Status is changed to Disabled.

Deselecting the device's OU

Use either the instructions for Classic or Absolute 7 depending on the setting that you see in the Absolute console.

- Deprovisioning Chromebooks - Absolute 7
- Moving the device to an unsynced OU
- Deselecting the device's OU
- Using the Unenroll Device Action

Deprovisioning Chromebooks

When you deprovision the Chromebook device in the Google Admin Console, Absolute retrieves the device's deprovisioned status during the next sync of the device and sets the device's Agent Status to Disabled.

For more information about Deprovisioning Chromebook devices, see Google Admin Console documentation.

Moving the device to an unsynced OU

An unsynced OU is an OU that isn't selected in Chromebook settings in the Absolute console.

To move the device to an unsynced OU:

1. Log in to the Google Admin console using the credentials for the account that you use to manage your devices.
2. From the Google Admin console home page, navigate to Devices > Chrome management > Devices.
3. On the navigation pane, search for and select the OU that contains the devices you want to unenroll.
4. In the Devices list, select the check box next to each device.
5. In the taskbar, click Move selected devices.
6. In the dialog that opens, select the unsynced OU you want to move the devices to and click Move.

The next time the device calls in, the device is unenrolled and the Agent Status is changed to Disabled.

Deselecting the device's OU

Use either the instructions for Classic or Absolute 7 depending on the setting that you see in the Absolute console.

- To deselect a device's OU - Classic
- To deselect a device's OU - Absolute 7
To deselect a device's OU - Classic:
1. Log in to the Absolute console as an Administrator.
2. On the navigation bar, click ✽ > Classic Account Settings.
3. Log in to the Absolute console as an Administrator.
4. In the Select Organizational Units dialog, deselect each OU containing the Chromebooks you want to remove from your Absolute account.

Absolute begins to update 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 in the Chromebooks - Google Account section of the Classic Account Settings page.

To deselect a device's OU - Absolute 7:

To deselect a device's OU:
1. Log in to the Absolute console as a user with Manage permissions for Policies.
2. On the navigation bar, click ✽ > Chromebook Settings.
3. On the sidebar, select the Google account that contains the Chromebooks that you want to unenroll.
4. In the work area, clear the selection for each OU that contains Chromebooks you want to unenroll.

After two seconds, your changes are automatically saved.

Devices are unenrolled and the Agent Status is set to Disabled for devices in the deselected OUs. Absolute schedules a sync with your Google account in 20 minutes time. The sync should take no longer than an hour. When this process is complete, the date and time are populated below the Google account in the sidebar in the Chromebook Settings page.

Using the Unenroll Device action

IMPORTANT If you unenroll your device using the Unenroll Device action, you will not be able to re-enroll your device without contacting support.

You can submit an Unenroll Device request to unenroll one or more devices from your account. For information on creating an unenroll request, see Unenrolling devices from your account in the online help.

Removing the Chromebook extension

As the Chromebook extension is a force-installed app that is available to all authorized users in your account, users cannot remove it from their device.

There are two ways to remove the Chromebook extension:

- Removing the Chromebook extension from all devices in an OU
- Removing the Chromebook extension from specific users
Removing the Chromebook extension from all devices in an OU

To remove the Chromebook extension for all users in a particular OU:
1. Log in to the Google Admin console using the credentials for the account that you use to manage your users.
2. From the Google Admin console home page, navigate to Devices > Chrome management > User & browser settings.
3. Select the OU that you want to remove the Chromebook extension from.
4. Scroll to the Apps and extensions section and click apps & extension page.
5. Click the Absolute for Chromebook app and click .
6. Click SAVE.

The Chromebook extension is removed from the list of force-installed apps for all users in this OU. When an authorized user logs in to the Chromebook, the extension is removed from the device.

Removing the Chromebook extension from specific users

By default, when an OU is configured for force-installed apps, all authorized users within the OU receive all apps. To remove the Chromebook extension for a specific user you need to move the user out of this OU.

To help with the removal of the Chromebook extension for specific users, we recommend that you set up at least one OU that does not have the Chromebook extension configured as a force-installed app. You can name the OUs accordingly, such as "No Absolute Extension".

You can then move users between OUs to manage the deployment of the Chromebook extension for individual users.

To remove the Chromebook extension from one or more authorized users:
1. Log in to the Google Admin console using the credentials for the account that you use to manage your users.
2. From the Google Admin console home page, click Users.
3. On the navigation pane, search for and select the OU that contains the users you want to update.
4. In the Users list, select the check box next to each user.
5. Click More > Change organizational unit.
6. In the dialog that opens, select the applicable OUs (for example, "No Absolute Extension") and click Continue.
7. On the User move confirmation dialog, click Change.

As the users log in to their Chromebooks, the extension is removed from each device.
Chapter 6: Testing network connectivity using the Network Diagnostics Tool

Use the Absolute Network Diagnostics Tool to test the network connectivity of your account's devices to the Absolute Monitoring Center. The Network Diagnostics Tool tests whether your device's Absolute agent connections are blocked or otherwise interrupted by your network's proxies and firewalls.

This section contains the following topics:

- Downloading the Absolute Network Diagnostics Tool
- Using the Network Diagnostics Tool

Downloading the Absolute Network Diagnostics Tool

➤ To download the Absolute Network Diagnostics Tool from the Absolute console:

1. Log in to the Absolute console as an Administrator.
2. On the navigation bar, click 📐.
3. On the Settings sidebar, click Download Packages.
4. On the Download Packages page under Network Diagnostics, click the Download Network Diagnostics Tool link to download the DDSNdt-<version>.zip file.
   Depending on your browser and operating system, you may need to click through several dialogs to download the .zip file to the location of your choice.
5. When the download is complete, extract the .zip file to the location of your choice. You can copy the files to the hard drive, or run them from a USB key or network drive as you need this file for the next task.

Using the Network Diagnostics Tool

You can run the Network Diagnostics Tool on each device that contains the Absolute agent to ensure uninterrupted connectivity of agent calls to the Absolute Monitoring Center.

➤ To use the Network Diagnostics Tool:

1. Open a Command Prompt window as a user with administrator permissions.
2. Navigate to the DDSNdt.exe file that you extracted in Downloading the Absolute Network Diagnostics Tool.
3. To run the Network Diagnostics Tool, enter one of the following commands:
   - To run the tool with the default data center location and to save the log file at the default location, enter DDSNdt.exe and then press ENTER on your keyboard. The Canadian data center is the default data center location. By default, the log file is saved in the working directory.
   - To run the tool with the US data center location, enter DDSNdt.exe /datacenter=US and then press ENTER on your keyboard.
   - To specify the location where the tool should save the log file, enter DDSNdt.exe /log=<add the new location where you want to save the log file> and then press ENTER on your keyboard.
For example, if you want to save the log file to a folder named NDTLogFile on your C: drive, enter DDSNdt.exe /log=c:NDTLogFile.

**IMPORTANT** The folder where you want to save the log file must exist on your device. If you want to use a new folder, you must create the folder first. Do not use special characters or spaces in the folder name.

- To view a help file showing the different options available for the tool, enter DDSNdt.exe /help and then press ENTER on your keyboard.

When the Network Diagnostics Tool finishes testing your device's connection, it saves the log file either to the default location or to the location you specified.

**Viewing the Network Diagnostics log file**

To view the log file, navigate to the location on your device where the tool saved the log file and double-click the log file to open it.

**HTTP status codes**

The log file may contain one or more HTTP status codes. See the following table for more information about the status codes included in the log file.

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>The request succeeded.</td>
</tr>
<tr>
<td>202 ACCEPTED</td>
<td>The request was accepted for processing, but the processing is not complete.</td>
</tr>
<tr>
<td>302 FOUND</td>
<td>The request resides temporarily under a different URL.</td>
</tr>
<tr>
<td>307 TEMPORARY REDIRECT</td>
<td>The request resides temporarily under a different URL.</td>
</tr>
<tr>
<td>401 UNAUTHORIZED</td>
<td>The request requires user authentication. The client needs to send the request with a suitable authorization header field.</td>
</tr>
<tr>
<td>403 FORBIDDEN</td>
<td>The server will not fulfill the request and it should not be repeated.</td>
</tr>
<tr>
<td>404 NOT FOUND</td>
<td>The server could not find the URL. The status does not indicate whether it is temporary or permanent.</td>
</tr>
</tbody>
</table>

**HTTP error messages**

If some requests fail, the log file may contain one or more HTTP error messages. For a complete list of HTTP error messages, refer to [https://docs.microsoft.com/en-us/windows/desktop/winhttp/error-messages](https://docs.microsoft.com/en-us/windows/desktop/winhttp/error-messages).

For details about additional error codes that may show in the log file, refer to the following table.

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>4317</td>
<td>Expired Token</td>
</tr>
<tr>
<td></td>
<td>The authentication token is invalid or expired. For assistance, contact Absolute Global Support.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 100100     | Deep Packet inspection detected  
The agent call failed due to a certificate host name error. |
| 100101     | Deep Packet inspection detected  
The agent call failed due to a certificate validation error. The pin is missing from the pinset or the pin value is blank. |
| 100103     | Deep Packet inspection detected  
The agent call failed due to a certificate validation error. The public key retrieved from the server doesn't match the pinned version of the public key. |
Glossary

A

Absolute
Absolute is technology that allows you to track and secure devices and the data they contain.

Absolute console
A web-based user interface that enables corporate customers to centrally manage all assets within the account.

Absolute Monitoring Center
A server with which the agent makes a secure connection to send device authentication and inventory data. The Monitoring Center is where devices call for self-healing.

activation
An event where a device contacts a Monitoring Center for the first time (over the Internet) to obtain a unique Identifier.

agent
A small software client that resides in the firmware or BIOS of a device. It’s either embedded at the factory or installed manually by a user. The agent makes regularly scheduled calls over the Internet to the Monitoring Center and provides identification points on each agent call. The agent also manages the programs that support activities such as Data Delete and Device Freeze.

agent call
A secure connection established by an agent to a Monitoring Center. During a call, the hardware profiles are sent to the Monitoring Center and instructions are sent to the device.

agent executables
Agent executables are used to install the agent on your managed devices and are unique to your account.

Agent Management utility
Part of the Absolute agent installation package and is also known as the DDSInfo or CTMWeb application, depending on the agent version. Facilitates managing individual agents and verifying an agent’s state.
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.

B

BIOS
Basic Input/Output System. Firmware embedded onto the system board of a computer.

BitLocker Drive Encryption (BitLocker)
BitLocker is a full-disk encryption feature included in most versions of the Windows operating system.

D

DDSGlobal
DDSGlobal Agent Management utility, an application that lets users verify and manage the Mac agent’s installation on a device.

device
A piece of electronic communication hardware, such as Windows or Mac computers, and Android smartphones, on which you can install the agent.

disk imaging
Used to copy standard applications onto unconfigured computers. Incorporating the agent Installer onto disk images helps to ensure that the agent is fully functional on all managed devices.

E

ESN
Electronic Serial Number. See also Identifier.

EvDO
Evolution Data Only.
F

**Firmware Persistence**

Most OEMs integrate Absolute’s Persistence technology within a computer’s firmware or BIOS, which is also known as hardware persistence. See Persistence technology.

**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. Absolute detects FDE Hardware (self-encrypting drives) and Software encryption programs that are installed on the hard drives of your organization’s managed devices.

G

**group**

A logical collection of devices based on criteria such as departments or geographical location. You can use the group to filter reports and target specific managed devices for many Absolute functions.

I

**ID**

Identification.

**Identifier**

A unique Electronic Serial Number (ESN) assigned to the agent installed on a device.

**IP**

Internet Protocol.

M

**managed device**

A device on which an Absolute agent is installed.

**Monitoring Center**

See Absolute Monitoring Center.
O

OEM
Original Equipment Manufacturer.

OS
Operating System.

P

Persistence module
The application embedded within the firmware or BIOS of a device. See Persistence technology.

Persistence technology
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.

S

SCCM
The Microsoft System Center Configuration Manager (SCCM) is a system management solution that allows organizations to manage installed software, compliance settings, and other services on a large group of servers, desktops, laptops, and mobile devices.

self-healing
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.

stamped agent
Embeds account and order specific information, namely the seed of an electronic serial number (ESN) into the package and also digitally signs the Windows installation package if an X.509.2 code signing certificate was originally entered using the Install wizard.

U

UMTS
Universal Mobile Telecommunications System.
USB

Universal Serial Bus.