Agent Install Guide

Absolute®Software

www.absolute.com

Agent Install Guide 5.4.5 - Documentation Release 1

Table of Contents

The Agent is a client software application that you install on the devices that you want to manage using Absolute Software services. Please visit www.absolute.com/en/products/computrace/features.aspx to see the current list of available services.

After installation, the Agent resides undetected on your device. The Agent contacts the Monitoring Center on a regular basis to report its location. The communication is quick, silent and requires no input from you.

The Agent does not affect system performance of your device or interferes with the Internet functions.

About This Guide

The Computrace Agent Install Guide contains the necessary instructions to install the Agent on your devices on various platforms.

The guide is organized as follows:

Audience

The Computrace Agent Install Guide is written primarily for users in the Administrator role in Customer Center to perform tasks, such as asset administration, device security, and data management.

Hardware and Software Requirements

Personal Computer Requirements

- Intel 486 or higher processor
- Supported Operating Systems
    - Windows 2000 Service Pack 4
    - Windows XP Service Pack 2 and higher (32-bit versions)
    - Windows Vista (32- and 64-bit versions)
    - Windows 7 (32- and 64-bit versions)
    - Windows Server 2003 (32-bit versions)
    - Windows Server 2008 (32- and 64-bit versions)
    - Windows Server 2008 R2
- Internet connection

Mac System Requirements

- PowerPC G3 or higher processor (including Intel)
- Internet connection or modem
- Mac OS X v10.4.9 or above

  NOTE Mac OS X v10.2 and earlier operating systems are not supported.

Linux System Requirements

- Intel based x86 processor
- 64 MB of system memory (RAM)
- Internet connection
- Supported Operating Systems
    - RedHat Enterprise Linux 5, Centos 5
    - Fedora 11 and 12
    - openSUSE 11.1 and 11.2
    - Debian 5.0.3
    - Ubuntu 8.04, 9.04, and 9.10
    - Mint 9.10

You can install the Linux Agent on both 32- and 64-bit hosts, provided the 64-bit host contains the 32-bit runtime support.

Contacting Global Support

If you have difficulty using or installing the Agent, please contact Absolute Software Global Support at http://www.absolute.com/support.

Follow on-screen instructions to contact technical support for your region. We welcome your questions, comments, and feature requests.

Chapter 2   # Installing the Agent on Windows Computers

This chapter provides instructions for the direct installation of the Agent on Microsoft® Windows computing assets. The direct installation method requires hands-on contact with each target computer and is commonly used to install the Agent on individual computers not connected via a network. For imaging instructions, please see <u>"Disk Imaging Windows and Mac Computers" on page 16</u>.

Before You Begin

IMPORTANT   Following these instructions ensures that the Agent remains tamper resistant.

To prepare for installing the Agent:

1. Use a virus-scanning program to ensure that your hardware is free from viruses.

2. If the computer is **not** using the BIOS Agent, list the primary hard drive first in the boot order specified in the BIOS.

3. Password protect the BIOS. Refer to your computer's documentation for more information.

4. Verify that the Internet connection on your computer is functioning correctly.

Installation Utility

To install the Agent on a Microsoft Windows operating system:

1. Double-click the .zip file containing the Agent installation package, and then extract the contents to a separate folder.

2. In the folder containing the installation package you extracted, double-click the file **Computrace.exe**.

3. Select the desired language in the drop-down menu

4. Click **Next** on the **Confirm Installation** dialog.

> OR

> Click **Cancel** to cancel the installation.

When installation is complete, the Agent contacts the Monitoring Center the next time the device connects to the Internet to receive an Identifier that uniquely identifies the computer.

See _"Forcing a Test Call" on page 13_ for more information about using the Agent Management utility to force a test call to the Monitoring Center.

NOTE On certain makes and models, a second call to the Monitoring Center is required to complete activation.

Installing the Agent Using the Command Line

You can also install the Agent on a Windows computer using the command prompt.

To install the Agent using the command prompt:

1. Double-click the ZIP file containing the Agent installation package, and then extract the contents to a separate folder.

2. Open a command prompt window and navigate to the location where you extracted the **Computrace.exe** file in step 1.

3. Depending upon the type of installation you need, type the following command with the desired switch:
   ```
   Run Computrace.exe
   ```

   NOTE See _"Installer Switches" on page 5_ for details about the switches available for the Agent installer.

   ---

4. Open the file. A security warning pop-up screen may appear to verify the publisher. If this happens, click **Run**.

5. The User Access Control window will open if you are using Windows Vista or higher. Click Yes to allow the setup program to make changes to your computer.

6. Select the appropriate language for installation.

7. The Agent installer runs according to the selected installer switch. And depending upon your specified preferences, on successful installation, the installer displays a confirmation message. The next step is to verify the installation of the Windows Agent. See _"Verifying the Installation" on page 5_ for information on how to verify a successful installation.

Installer Switches

You can run the Agent installer using specific commands known as "switches". Installer switches allow you to launch the installer in a specific mode, using a specific interface. The following switches are available with the Agent installer.

Table 1. Installer Switches*

Switch	Description
-sp/s	Silent install mode.
-sp/s / f2"C:\Setup.log"	Silent install mode with log file.

* See the following link for more information:
http://kb.flexerasoftware.com/doc/Helpnet/installshield12helplib/lHelpSetup_EXECmdLine.htm.

Verifying the Installation

To verify that the Agent has successfully contacted the Monitoring Center and received a unique Identifier, follow these steps:

1. Using Windows Explorer, browse to the folder containing the Agent installation package you extracted.

2. Double-click the file **CTMWeb.exe** to launch the Agent Management utility. The CTMWeb Login page opens.

3. In the **Please enter your password** field, type the administrative password set after installation, and then click **Next**. By default, the out-of-the-box password for the Agent Management utility is **password**

4. To verify successful Agent installation, review the following fields:

   ○ **Agent Mode** — Confirm that the value is **Active**.

   ○ **Identifier** — For activated Agents, the last four characters of the Identifier are greater than 0000. If the last four characters are zero, click the **Test Call** tab in the Agent Management utility and

then click the **Start** button to force a test call to the Monitoring Center. Call status displays on screen.

IMPORTANT **Last IP Call Date/Time** — When the Monitoring Center successfully receives a call from the Agent, the value is updated. Displaying a date value indicates a successful call. If the field is empty, your computer has failed to contact the Monitoring Center. Review the installation steps to ensure no steps are missed. If the Agent still cannot contact the Monitoring Center, contact Absolute Software Global Support at http://www.absolute.com/support. By default, the Agent is installed with modem support disabled. The modem is automatically enabled on stolen machines during the first post-theft call to the Monitoring Center. For this reason, most computers display "`No last call`" in the **Last Modem Call Date/Time** field.

STATUS | **TEST CALL** | **OPTIONS** | **ABOUT**	English ▼

STATUS

CTMWeb Build #	881
Agent build #	879
Agent mode:	Active
ESN:	4EA739AA63FV0KWD2130
Last IP Call Date/Time:	11/17/2008 9:56 AM
Next IP Call Date/Time:	11/18/2008 10:26 AM
Last Modem Call Date/Time:	No last call
Next Modem Call Date/Time:	11/24/2008 9:56 AM
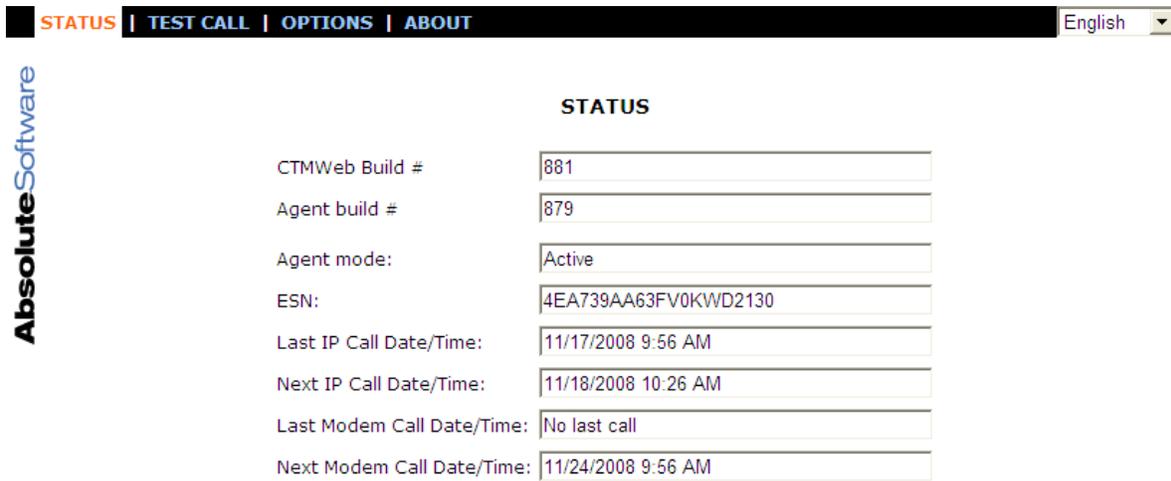
FIGURE 1. CTMWeb Status Page

NOTE On devices running a Microsoft Windows operating system, you cannot remove the Agent using Customer Center or tools in the installation package. If you need to remove the Agent, contact Absolute Software Global Support. See "Contacting Global Support" on page 2.

Default settings apply during Agent installation. After installation, you can modify Agent settings for individual computers locally using the Agent Management utility. For full details on using the Agent Management utility, see "Managing the Agent" on page 11.

Chapter 3   # Installing the Agent on a Mac

This chapter provides instructions for installing the Computrace® Agent on a Mac® device. The installation methods described in this chapter require hands-on contact with target devices that are not usually connected to a network.

System Requirements

- Internet connection or modem
- Mac OS X v10.5.8 or above

  NOTE Previous versions of Mac OS X operating systems are not supported.

Before You Begin

Before you install the Agent on a Mac device, ensure the following for your device:

- the Internet connection is functioning properly.
- you have local administrator rights.
- your hard drive is clean of viruses after scanning the device with a anti-virus program.
- you have disabled all resident virus-scanning programs.

  IMPORTANT Re-enable all virus-scanning programs upon completing the Agent install process.

- you have made a note of all details of your device, including make, model, and serial number.

Installing the Agent Using the Installation Utility

You can find the Agent installation utility in the **CTClientxx-yy.zip** file where **xx** is your account number and **yy** is the order number.

To access the Agent installation utility:

> ➢ Browse to the location of the .zip file and double-click it. The Agent installation folder is extracted and saved in the same location.

> **NOTE** The **CTClientxx-yy.zip** archive also contains the Installation Guide and the Release Notes.

You can use one of the following methods to install the Agent on a Mac device:

- Using the Installation Package

- Using the Command Line

Using the Installation Package

To install the Agent using the installation package:

1. Browse to the Agent installation folder and double-click **rpclient.tar** to extract the contents of the archive.

   The **rpclient.pkg** file is extracted and saved in the same folder location.

2. Double-click the **rpclient.pkg** file to open the Install Computrace Agent page.

3. Click **Continue**.

4. Click **Install** to perform a standard installation of the Agent, and to open the password dialog.

   > **NOTE** If you want to change the default installation folder on your device, click **Change Install Location**.

5. In the **Password** field, enter the Mac Administrator password on your local device and click **Install Software**. You receive notification that confirms a successful installation.

6. Click **Close**.

Using the Command Line

To install the Agent on a Mac device using the command line:

1. Browse to the Agent installation folder and double-click **rpclient_image.tar** to extract the contents of the archive.

   The **Install** folder is extracted and saved in the same folder location.

2. Open a **Terminal** window, and then browse to the Agent installation folder.

3. Type **sudo ./install.sh** to run the installation package with full security privileges.

4. When prompted, type your Mac Administrator password for the local device, and then press **ENTER**.

5. When the following message shows, the Agent is installed on the device:
    ```
    Install path is: /<install path>

    You may now create a drive image with computrace agent
    on the first startup from the imaged drive, the
    installation will complete
    ```

6. Reboot the device.

Verifying the Installation

To verify that the Agent has contacted the Monitoring Center successfully and received a unique Identifier, perform the following steps:

1. Browse to the Agent installation folder and double-click **ctm.tar** to extract the contents of the archive.

    The **ctmweb** file is extracted and saved in the same folder location.

2. Double-click the **ctmweb** file to start the Agent Management utility. The CTMWeb Login page opens.

3. Click **Manage**.

4. In the **Please enter your password** field, type **password**, which is the default password for managing the Agent, and click **Next**.

    > **IMPORTANT** See "Changing the Default Password" on page 10 for more information on how to change the default password.

5. To verify successful Agent installation, confirm the following fields:

    ○ **Agent Mode** — the value is **Active**.

    ○ **Identifier** — the last 4 characters of the Identifier are greater than 0000.

        > **IMPORTANT** If the last 4 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. Call status shows on screen. If the call is successful, the last 4 characters are greater than 0000.

○ **Last IP Call Date/Time** — The field shows an appropriate time and date, instead of the **No last call** value.

NOTE After successful installation, you can remove the Agent or modify Agent settings for individual devices locally by using the Agent Management utility. See "Managing the Agent" on page 11 for full details.

Changing the Default Password

You can change the default password for managing the Agent to increase security.

To change the default password:

1. Browse to the Agent installation folder.

2. Double-click the **ctmweb** file to start the Agent Management utility. The CTMWeb Login page opens.

3. Click **Manage**.

4. In the **Please enter your password** field, type the current password and click **Next**.

5. Click the **Options** tab.

6. In the **New Password** and **Confirm Password** fields, enter the new password.

7. Click **Apply**.

Chapter 4   # Managing the Agent

The Absolute Agent installation package includes the CTMWeb tool to facilitate management of individual Agents. Use the Agent Management utility to verify the state of the Agent in an image before deploying the image to machines in your network.

You can perform the following administrative tasks using the Agent Management utility after Agent installation:

- Forcing a Test Call
- Configuring IP Proxy Settings
- Upgrading the Agent Version

You can perform the following additional tasks on Macintosh computers:

- Upgrading the Agent Version
- Removing the Agent

Launching the Agent Management Utility

The Agent installation package includes two files **CTMWeb.exe** and **CTMWeb.xsl**. To launch the Agent Management utility, follow the procedure for your operating system.

On a Windows Computer

IMPORTANT To manage the Agent, you must have Administrator credentials if User Access Control is enabled.

To launch the Agent Management utility on a Windows computer:

1. Using Windows Explorer, browse to the folder containing the Agent installation package you extracted when installing the Agent. See "Installation Utility" on page 3.

2. Double-click the file **CTMWeb.exe** to launch the Agent Management utility. The CTMWeb Login page opens.

3. In the **Please enter your password** field, type the administrative password set after installation, and then click **Next**. By default, the out-of-the-box password for the Agent Management utility is **password**.

On a Mac Computer

The Agent Management utility exists in the Desktop installation package. Installing the Agent does not create another copy on the computer.

IMPORTANT   The Agent Management utility includes functionality to remove the Agent. Therefore, Absolute Software recommends that you remove the installation files from the local computer after management tasks are complete.

To launch the Agent Management utility manually:

1. Extract the **ctm.tar** archive from CTClient*xx-yy*.zip.

2. In the **ctm** folder, double-click the file **ctmweb**.

3. Click the **Manage** button.

4. In the **Please enter your password** field, type the password for managing the Agent, and then click **Next**.

On a Linux Computer

The installation files for Linux computers are delivered in a ZIP archive CTLinuxXX-YY.zip. The installation process for Linux is a manual process. See Chapter 4 "Installing the Agent on Linux Computers" on page 10 for more information.

IMPORTANT   Absolute Software recommends that you remove the installation files from the local computer after management tasks are complete.

Viewing Agent Call Details

Figure 1, "CTMWeb Status Page," on page 6 shows the Agent Management utility Agent Status page. The Status page displays the following fields:

- **CTMWeb Build #** — Version number of the CTMWeb application

- **Agent Build #** — Version number of the Agent installed on the computer

- **Agent Mode** — State of the installed Agent, displaying the following possible values:

  - `Active` — The Agent is installed and active.

  - `Call Support` — A problem exists with the Agent. Please use the information provided in "Contacting Global Support" on page 2.

- **Identifier** — Unique Electronic Serial Number assigned to the installed Agent

- **Last IP Call Date/Time** — Date and time of the last successful Agent call using Internet Protocol from the local computer to the Monitoring Center

- **Next IP Call Date/Time** — Date and time of the next scheduled call via Internet Protocol from the Agent on the local computer to the Monitoring Center

- **Last Modem Call Date/Time** — Date and time of the last successful Agent call via modem from the local computer to the Monitoring Center

- **Next Modem Call Date/Time** — Date and time of the next scheduled call via modem from the local computer to the Monitoring Center

Forcing a Test Call

To request that the Agent contact the Monitoring Center immediately, use the Test Call page.

To make a test call:

1. Connect the computer to the Internet.

2. In the Agent Management utility, click the **Test Call** tab.

3. Click the **Start** button.

The Agent attempts to contact the Monitoring Center. The **Call Status** field displays progress information.

NOTE The screen may flicker.

To verify the success of a test call:

➢ On the Status page in CTMWeb, review the **Last IP Call Date/Time** and **Last Modem Call Date/Time** fields. If either field displays the current date and time, the call succeeded. Also, successful calls update the **Next IP Call Date/Time** or **Next Modem Call Date/Time** field depending on the connection used to contact the Monitoring Center.

Configuring IP Proxy Settings

IMPORTANT This functionality is not supported on Linux computers.

The Agent can access the Internet via a proxy server to contact the Monitoring Center.

To set the account used to access a proxy server:

1. In the Agent Management utility, click the **Options** tab.

2. In the **Name** field, type the user name for the Agent to access the Internet via proxy server.

3. In the **Password** field, type the password for the Agent to access the Internet via proxy server.

4. To save changes, click the **Apply** button at the bottom of the page.

To confirm that the Agent is functioning correctly using the new settings, make a test call to the Monitoring Center. See <u>"Forcing a Test Call" on page 13</u>.

Upgrading the Agent Version

> **IMPORTANT** The Agent Management utility for Windows and Linux does not allow upgrading the Agent version from the local computer.

To upgrade the Agent version installed on a Mac:

1. In the Agent Management utility, click the **Options** tab.

2. In the **Enter Mac Admin password** field, type your Administrator password for the local computer.

3. Click the **Upgrade Version** button.

The Agent Management utility for Mac downloads the latest Agent version from the Monitoring Center and replaces the Agent installed on the Mac, preserving all settings.

Removing the Agent

As a computer population ages, some devices are retired or destroyed. Similarly, the Identifiers associated with these devices should be retired. Retired (or disabled) Identifiers no longer consume a license, and do not appear in Customer Center reports unless specifically selected.

Identifiers are assigned to a single device, and are not reusable. However, the license associated with a retired Identifier can be applied to a new Identifier. You can disable an Identifier using Customer Center, but this does not remove the Agent from the device.

To retire Identifiers and remove the Agent from a device, contact Absolute Technical Support and notify us of the Identifier(s) you wish to retire. Absolute then marks the Identifiers as 'disabled' removing the Identifier from most Customer Center reports, and instructing the device to cease calling the Monitoring Center.

You can periodically e-mail Absolute the list of Identifiers you wish to retire. Please contact Absolute's Technical Support team to determine the required file

format and an appropriate schedule. See for more information on how to contact Absolute Software Global Support.

> **NOTE** Once an Identifier has been retired (disabled), it can only be re-enabled by advising Absolute and reinstalling the Agent.

Follow the procedure specific to your computer and Operating System to remove the Agent.

On a Windows Computer

To remove the Agent:

> ➢ Contact the Absolute Software Global Support team at http://www.absolute.com/support.

On a Macintosh Computer

If you use a Macintosh computer and you have access to the device, the Agent Management utility for Mac includes functionality to remove the Agent from the local computer.

To remove the Agent from a Mac locally:

1. In the Agent Management utility, click the **Remove** tab.

2. In the **Enter Mac Admin password** field, type your Administrator password for the local computer, and then click **OK**.

3. To confirm that you want to delete the Agent, click **OK**.

The Agent Management utility removes the Agent from the local computer and displays a message confirming that the Agent is removed. Close the browser window.

On a Linux Computer

To remove the Agent:

> ➢ Contact the Absolute Software Global Support team at http://www.absolute.com/support.

Chapter 5

Disk Imaging Windows and Mac Computers

Disk imaging is used to copy standard applications onto unconfigured machines. Incorporating the Agent installer into disk images helps ensure that the Agent is fully functional on all managed devices.

First, a single computer (the source computer) is configured with all of the company's desired software. Then, an imaging program is used to create a complete image of the computer's hard drive. Finally, this disk image is copied to any number of identical systems (the target computers).

To install the Agent using imaging, disconnect wired and wireless network connections on the source computer, and then prepare the computer with all desired software, including the Agent software. Disconnecting the computer from the network ensures that the Agent does not activate. With the machine still disconnected from the network, image the machine's hard drive. Images created in this manner initially display a generic Identifier that is associated with your account. When deployed, each target computer contacts the Monitoring Center on its first boot and receives a unique Identifier.

IMPORTANT Ensure that you do not create the installation image from a computer on which the Agent is active. Copying an image having an active Agent installation to multiple computers may result in multiple machines having the same Identifier. Subsequently, there is no way of differentiating between the machines because each contacts the Monitoring Center using the same Identifier.

If you want to create an image using a computer that supports BIOS persistence, BIOS persistence on the computer must be disabled. If BIOS persistence is enabled from a prior Agent activation, contact Global Support to disable the BIOS persistence temporarily while you create the image.

Creating Disk Images For Windows Computers

Before You Begin

To prepare for creating a disk image:

1. Use a virus-scanning program to ensure that your hardware is free from viruses.

2. If the computer is **not** using the BIOS Agent, list the primary hard drive first in the boot order specified in the BIOS.

3. Password protect the BIOS. Refer to your computer's documentation for more information.

4. Prior to installing the Agent when configuring the disk image, verify that the Internet connection on your computer is functioning correctly.

5. After installing the Agent and prior to creating the image, use the Agent Management utility to verify that the password is set correctly (the default password is **password**) and the Electronic Serial Number (ESN) ends in four zeros.

6. For security reasons, if installed locally delete the Computrace Agent Management utility having the file name **CTMWeb.exe** from the computer prior to creating the image.

Creating the Standard Image

Follow the steps below to create a standard drive image for a Windows computer.

1. **Prepare the Source Computer** — Starting with a freshly formatted computer, install an operating system and any desired software to be included in the image. Absolute recommends that you install the Agent last. Disconnect the computer from the network, and then install the Agent.

    IMPORTANT   Ensure the source computer does not have internet connectivity when you install the Agent. Disable wired and wireless connections.

    Once installed on the source computer, the Agent attempts to contact the Monitoring Center to receive a unique Identifier. It is imperative that the Agent not be able to secure a unique Identifier prior to the creation of the image.

2. **Create An Image** — With the computer still disconnected from the network, create a hard drive image of the source computer.

3. **Test The Image** — Deploy the drive image to a target computer, connect the target to the internet and verify the target's Agent has received a unique Identifier. To verify the Agent's Identifier, see "Verifying the Installation" on page 5.

Using a Batch File to Install the Agent

Instead of installing the Agent manually prior to creating a disk image, you can use a batch file to install the Agent automatically the first time a computer boots after restoring the disk image.

To implement a batch file Agent installation in your disk image:

1. Copy the file **Computrace.exe** to the root folder of drive **C:**.

2. Create a file having the name **ct.bat** that contains the following commands:

   ○ For Windows 2000, XP, and 2003:

   ```
   @echo off

   Computrace.exe -sp/s

   del C:\Computrace.exe

   del "C:\Documents and Settings\All Users\Start
   Menu\Programs\Startup\ct.bat"
   ```

   ○ For Windows 2000, XP, and 2003:

   ```
   @echo off

   Computrace.exe -sp/s

   del C:\Computrace.exe
   ```

   IMPORTANT For Windows Vista, 7, and 2008, run the installer as an administrator.

3. Save **ct.bat** in the Startup folder.

   NOTE Depending upon the version of Windows on the device, the location of the Startup folder changes. Refer to the *User Guide* or *Online Help* for the version of Windows you are running.

4. Create the disk image before you reboot the computer.

Creating Disk Images for Macs

Follow the steps below to create a standard drive image for a Mac computer.

1. **Prepare the Source Computer** — Starting with a freshly formatted computer, install the operating system and any desired software to be included in the image.

2. **Extract the contents of the rpclient_image.tar archive** — From the installation media, extract the contents of *rpclient_image.tar* to the local machine and note where the files are located.

3. **Navigate to the installation directory** — Open a terminal window and navigate to the directory where you extracted the files in Step 2.

4. **Run the installer** — Enter the following command
   `sudo ./install.sh`

   When prompted, enter the administrative password. The installation completes and the following confirmation message displays:

   ```
   Install path is: /
   You may now create a drive image with the Agent. On
   the first startup from the imaged drive, the
   ```

```
installation will complete.
```

5. Create an image of the hard drive.

6. Test the new hard drive image. Deploy the drive image to a target computer, connect the target to the internet and reboot the machine. Verify the target's Agent has received a unique Identifier. To verify the Agent's Identifier, see "Verifying the Installation" on page 9.

Chapter 6 ## Installing the Agent on Windows Mobile Devices

This chapter provides instructions for installing the Mobile® Agent on Windows Mobile devices.

Supported Operating Systems and Devices

The Mobile Agent supports all makes and models of Smartphones and Pocket PCs on the following operating systems:

- Windows Mobile 5.0, 6.0, 6.1 and 6.5

> **NOTE** Windows Mobile 5.0 devices require an installation of the .NET Compact Framework 2.0 SP2 Runtime, available from Microsoft at: http://www.microsoft.com/downloads/details.aspx?FamilyID=aea55f2f-07b5-4a8c-8a44-b4e1b196d5c0&displaylang=en

Downloading the Installation Package

The Mobile Agent installer is available on the **Download Packages** page in Customer Center. The installation package is in Windows ZIP format. The ZIP file contains the following two (2) separate Windows CAB (cabinet) files — one settings file and one individual file for each supported type and operating system.

- **ComputraceMobile_WM_2_0.CAB** — containing the Agent and Dashboard for Windows Mobile Smartphones
- **ComputraceMobile_Settings.CAB** — containing the configuration file common to all Windows Mobile devices

To download the installation package:

1. Log in to Customer Center. The Home Page appears.
2. Click the **Download Packages** link on the Home Page.
3. On the **Download Packages** page, click the **Windows Mobile** link in the **Agent Type** column of the **Agent** table.
4. Save the installation package (ZIP file) to your local computer.
5. Double-click on the ZIP file and extract the two CAB files to a local folder.

Installing the Mobile Agent

1. Copy the **ComputraceMobile_Settings.CAB** file and the **ComputraceMobile_WM_2_0.CAB** file to your Windows Mobile device. This can be done by:

   ○ Cradling the device and copying the CAB files

   ○ Sending the files to the phone by e-mail

2. Navigate to the location of the two CAB files on your Windows Mobile device.

3. Double-click on the **ComputraceMobile_Settings.CAB** file. The configuration settings specific to your account are installed on the device. When the installation is complete, a confirmation message displays.

4. Double-click on the CAB file containing the Mobile Agent and the Control Panel applet. The Agent and the Control Panel applet are installed on the device. When the installation is complete, a confirmation message displays.

Using the Dashboard

Once Computrace Mobile is installed, you can use the Dashboard Application to verify your installation, view information about the Agent, and place test calls.

The installer adds a link to the Start Menu called **CT Dashboard** providing quick access to start the dashboard application. On Windows Mobile 6.5 devices, the **CT Dashboard** link appears at the bottom of your TouchFlo^{TM} interface.

Setting Your Password

The first time you run the Dashboard application, you are prompted to enter a password. The password must be at least six (6) characters long.

Viewing Information about the Agent

To view information about the Agent:

1. Tap the **Computrace Agent** icon.

2. When prompted, enter your password.

3. Tap **Login**. The status page appears.

The status page lists the following information:

• **Agent Version** — Agent version number

• **Identifier** — Electronic Serial Number of device (unique identifier)

- **Next Call** — date and time of next scheduled call from device
- **Last Call** — date and time of last call from device
- **Call Status** — Agent state (e.g. Active)
- **Last Call Status** — Status of the last call (e.g. None, Completed Successfully)

Placing a Test Call

To place a test call:

➢ Tap the **Make Test Call** link text (or select the **Make Test call** from the menu). The Windows Mobile device calls the Monitoring Center.

Changing Your Password

To change your password:

1. Tap the **Options** menu and select **Change Password** from the list of choices.
2. Enter your new password in the **Password** and **Confirm Password** box.
3. Tap **Submit**.

Chapter 7   *Using the Agent on BlackBerry Devices*

This chapter provides instructions for installing, using and uninstalling the Mobile Agent on Research in Motion (RIM®) BlackBerry® smartphone devices.

Introduction

The agent has two main deployment paths:

- **To individual devices** using BlackBerry Desktop Software via USB cable
- **To multiple devices** via application policies set on a BlackBerry Enterprise Server (BES)

Supported Devices

The Mobile Agent supports devices running BlackBerry OS version 4.2.1 or higher.

Software Components

The Mobile Agent uses two main deployable applications:

- **Launcher** downloads and updates the Mobile Agent software as needed. The Agent application silently collects data to identify and locate the asset, and contacts the Absolute Software Monitoring Center using TCP/IP daily.
- **Dashboard** displays Agent status and allows you to place a test call to the Monitoring Center. The dashboard application is optional. The Agent can function without the Dashboard.

The Mobile Agent Bundle for BlackBerry devices that you require for installation is available from the Download Packages page in Customer Center as a ZIP archive. The root folder of the archive contains the following folders and files:

- rlsnotes.txt
- Launcher folder containing the following files:
    - Computrace_Mobile_Launcher_for_BlackBerry_v1.2.alx
    - com_absolute_apputils_1_2.cod
    - com_absolute_esn.cod
    - com_absolute_launcher_1_2.cod
    - com_absolute_ws_1_2.cod

- Launcher_and_Dashboard folder containing the following files:

    - Computrace_Mobile_Launcher_and_Dashboard_for_BlackBerry_v1.2.alx

    - com_absolute_apputils_1_2.cod

    - com_absolute_dashboard_1_2cod

    - com_absolute_esn.cod

    - com_absolute_launcher_1_2.cod

    - com_absolute_ws_1_2.cod

NOTE The Mobile Agent Bundle for BlackBerry devices does **not** include the Mobile Agent. The Launcher downloads and updates Agent software as needed. Devices always receive the latest Agent version. BlackBerry Enterprise Servers can enforce Launcher installation using a policy.

Using BlackBerry Desktop Software

Before beginning the installation, you need:

- Mobile Agent Bundle for BlackBerry devices

- BlackBerry Desktop Software

- Supported BlackBerry device

- USB cable

To install the Mobile Agent using BlackBerry Desktop Software:

1. Extract all files from the Mobile Agent Bundle for BlackBerry devices ZIP archive to a temporary directory.

2. Download and install the latest version of BlackBerry Desktop Software from RIM at http://us.blackberry.com/apps-software/desktop/.

3. Connect your BlackBerry device to your computer using a USB cable.

4. Once the device successfully connects, the BlackBerry Desktop Software home page opens to display a snapshot of the handset, including some or all of the following details:

    - Model name

    - Personal Identification Number (PIN)

    - Phone Number

    - Device software version

    - Last sync (date and time)

    - Last backup (date and time)

5. On the left hand navigation bar, click **Applications**, and then click the **Start** button in the **Add / Remove Applications** area.

6. In the **Device Application Selection** dialog, click the **Import Files** button. The **File Open** dialog appears.

7. To install the Launcher only, select the file **Computrace_Mobile_Launcher_for_BlackBerry_v1.2.alx** that you extracted in <u>step 1</u>.

OR

To install the Launcher and Dashboard, select the file **Computrace_Mobile_Launcher_and_Dashboard_for_ BlackBerry_v1.2.alx** that you extracted in <u>step 1</u>.

8. In the list of applications, click the ▢ button next to the application you want to add.

9. At the bottom of the screen, click the **Apply** button. The download of the BlackBerry Desktop Software starts. Once download is complete, the Mobile Agent is installed to the BlackBerry device. Once installation is complete, the device may restart.

IMPORTANT After the Launcher downloads the most recent Agent version for your device, you may see the error message **ControlledAccessException: Interprocess Communication** followed by a prompt to restart. This is normal during the Agent upgrade process and may also happen in the future when Absolute Software publishes Mobile Agent updates.

Using BlackBerry Enterprise Server

NOTE For a general information on deploying applications with BlackBerry Enterprise Server, see "Preparing to distribute BlackBerry Java Applications" in the BlackBerry Enterprise Server Administration Guide available at: <u>http://docs.blackberry.com/en/admin/deliverables/16606/ Preparing_to_distribute_BB_Java_Apps_579016_11.jsp</u>.

Before beginning the installation, you require:

• Mobile Agent Bundle for BlackBerry devices

• BlackBerry Enterprise Server v5.0.1 or later implementation

• Supported BlackBerry devices registered on your BlackBerry Enterprise Server

To install the Mobile Agent using BlackBerry Enterprise Server:

1. Download the **Mobile Agent Bundle for BlackBerry devices** from Customer Center and save it to a folder on your local hard drive.

2. Extract all files from **the Mobile Agent Bundle for BlackBerry devices** ZIP archive to a temporary directory. The ZIP archive contains two folders, namely, **Launcher** and **Launcher_and_Dashboard**. To install

the Launcher application only, see step 3. To install the Launcher and Dashboard, see step 4.

3. To install the Launcher only:

    a) Select all the files from the **Launcher** subfolder in the temporary directory.

    b) Right-click the selected files, and then select **Send to > Compressed (zipped) Folder**. The newly created ZIP archive is available in the Launcher subfolder and is necessary for deploying the Mobile Agent using BES.

        > **NOTE** If necessary, rename the auto-generated ZIP archive to **Computrace_Mobile_Launcher_vX.x.zip**, for easier retrieval during BES deployment.

    c) See step 5 for further instructions.

4. To install the Launcher and Dashboard:

    a) Select all the files from the **Launcher_and_Dashboard** subfolder in the temporary directory.

    b) Right-click the selected files, and then select **Send to > Compressed (zipped) Folder**. The newly created ZIP archive is available in the Launcher subfolder and is necessary for deploying the Mobile Agent using BES.

        > **NOTE** If necessary, rename the auto-generated ZIP archive to **Computrace_Mobile_Launcher_and_Dashboard_vX.x.zip**, for easier retrieval during BES deployment.

    c) See step 5 for further instructions.

5. Logon to the BlackBerry Enterprise Server administration console.

6. In the BlackBerry solution management pane available on the left hand navigation menu, click **Software** > **Applications** > **Add or update applications**. The Add or update applications page opens.

7. Click the **Browse** button to open a file open dialog.

8. In the **file open** dialog, browse to the folder on your local hard drive containing the desired ZIP archive, and click the file to select it. The Server file path and file field now displays the file path and location of the ZIP file.

9. Click the **Next** link to add the selected application to the BES. The Add or update applications page refreshes to display the details about the application added.

10. Click the **Publish application** link to publish the selected application to the BES. The Add or update applications page refreshes to display a confirmation message that selected applications were successfully published and a table listing details about the applications published.

11. In the **Application name** column, click the desired **application name** link to open the Manage applications page for the application.

> **NOTE** You can also access the Manage applications page, by clicking **Software** > **Applications** > **Manage applications** on the left hand navigation menu.

12. In the **Application versions** table, click the desired **version number** link to display more details about the desired version of the application.

13. Click the **Application control policies** tab.

14. Click the Edit application link. The Manage applications page refreshes to display two additional options.

15. In the **Settings** box, select the **Use custom application control policies** option. The page refreshes to display a table displaying settings for each item in the application control policy.

16. Set the access permissions for the following items in the application to **Allowed**:

   ○ Is access to the interprocess communication API allowed

   ○ Are internal network connections allowed

   ○ Are external network connections allowed

   ○ Is access to the phone API allowed

   ○ Is access to the email API allowed

   ○ Is access to the PIM API allowed

   ○ Is access to the handheld key store allowed

   ○ Is access to the GPS API allowed

   ○ Is access to the file API allowed

   ○ Is access to the module management API allowed

   ○ Is access to the WiFi API allowed

   ○ List of internal domains - set to **absolute.com**

   ○ List of external domains - set to **absolute.com**

> **NOTE** You can retain the settings for all other items at the default values. If you are in doubt, set the access permissions for all items to **Allowed**.

17. Return to the top of the page, and type desired values in the **Required application control policy name** and **Description** text boxes.

18. Click the ▢ button to add the custom application control policy to the list of policies available in BES. The policies table refreshes to a list of all

the custom policies available in BES and a blank policy with the values set to default.

> **NOTE** To edit the new custom policy, click the ▢ button to open the policy in editing mode.

19. Scroll to the bottom of the page, and click the **Save all** link. The Manage applications (summary) page displays listing the new application control policy.

20. On the left hand navigation menu, click **Software** > **Manage software configurations**. The Manage software configurations page opens to display a list of all software configurations available in BES.

21. In the table, click the desired **software configuration name** where you want to add the Computrace Mobile application. The Manage software configurations page refreshes to display detailed information about the software configuration selected.

22. Click the **Applications** tab.

23. Click the ▢ button to open the software configuration for editing. The Manage software configurations page refreshes to display editable fields.

24. Scroll down the page to the **Computrace Mobile Launcher and Dashboard** check box, and select the check box.

25. In the **Disposition** list, select **Required**.

26. In the **Deployment** list, select **Wireless**.

27. In the **Application control policy** list, select the name of the custom application control policy you created in step 17 using the Manage applications page.

28. Click the ▢ **Add to software configuration** button to add the values to the software configuration. The Manage software configuration page opens with the changes added to the software configuration.

29. Click the ▢ **Save all** button. The Manage software configuration page refreshes to display the Computrace Mobile application in the **Required application name** tab.

30. Use the Manage users and Manage groups pages to add the software configuration to a user or user group and Computrace Mobile deploys to the selected users and groups at the next opportunity.

For further assistance delivering the Mobile Agent using BlackBerry Enterprise Server, see "Preparing to distribute BlackBerry Java Applications" in the BlackBerry Enterprise Server Administration Guide available at: http://docs.blackberry.com/en/admin/deliverables/16606/ Preparing_to_distribute_BB_Java_Apps_579016_11.jsp.

IMPORTANT Performing Data Delete operations on devices activated using BlackBerry Enterprise Server having Wireless Sync capabilities deletes information on the device as well as the synchronizing Exchange or Lotus server. Before executing a Data Delete command on a BlackBerry device, ensure that you back up all relevant sensitive data on the Exchange or Lotus server.

Required Permissions

You need to set application permissions so that the Mobile Agent can operate without prompting the user. Asset Tracking and Data Delete functionality also requires setting permissions for the Web Services module.

To set application permissions for the Mobile Agent on BlackBerry devices:

1. On the BlackBerry device, click the **Applications** icon on the Desktop, then click **Options**, then click **Advanced Options**, and then click **Applications**.

2. Select **Computrace Mobile Launcher**.

<div align="center">OR</div>

   Select **Computrace Mobile Launcher and Dashboard**.

3. Press the **Menu** button, and then click **Edit Permissions**. Set permissions to match Appendix B "BlackBerry Application Permissions for the Mobile Agent" on page III.

4. Click the **Back** button, then click **Save**, then click the **Menu** button, and then click **Modules**.

5. Select the Web Services module named **com_absolute_ws_1_2**, press the **Menu** button, and then click **Edit Permissions**.

6. Ensure that permission for **Carrier Internet** is set to **Allow**, and then save any changes.

Removing the Mobile Agent

Depending on your needs, you can remove the Mobile Agent from BlackBerry devices using Desktop Manager or Enterprise Server.

Using BlackBerry Desktop Software

To remove the Mobile Agent using BlackBerry Desktop Software:

1. Connect your BlackBerry device to your computer using a USB cable.

2. In BlackBerry Desktop Software, ensure that your device is connected and your Personal Identification Number (PIN) appears in the bottom left corner.

3. Click **Application Loader**, and then click the **Start** button in the **Add / Remove Applications** area.

4. In the **Device Application Selection** dialog, deselect **Computrace Mobile Launcher**.

<div align="center">OR</div>

Deselect **Computrace Mobile Launcher and Dashboard**.

5. Click **Delete**. In the **Summary** dialog, ensure that information is correct, and then click **Finish**.

Using BlackBerry Enterprise Server

To remove the Mobile Agent using BlackBerry Enterprise Server:

1. In the BlackBerry Manager application, click **BlackBerry Domain** in Explorer View, and then click the **Software Configurations** tab. Right-click on white space in the pane listing configurations, and then click **Manage Application Policies**.

2. Select the policy for the Mobile Agent, and then click the **Properties** button.

3. Set the **Disposition** property to **Disallowed**, and then click **OK** two times.

Within four hours, BlackBerry Enterprise Server removes the Mobile Agent from BlackBerry Devices activated using BES.

Troubleshooting

To troubleshoot a Mobile Agent installation on a BlackBerry device, follow these general steps:

1. Ensure that the Launcher downloaded and installed the Mobile Agent.

2. Inspect Launcher code modules.

3. Confirm that Launcher permissions are correct.

4. Verify the status of data connections.

5. Perform a reset on the device.

See the following sections for a detailed discussion.

Investigating Agent Download

When you install the Mobile Agent, if a data connection is available the Launcher contacts the Absolute Software Monitoring Center within 10 minutes to download the latest Mobile Agent version for your device.

To investigate Mobile Agent download and installation:

1. On the BlackBerry device, navigate to the list of modules for the Mobile Agent. See _"Required Permissions" on page 29_ for more information on accessing the list of modules.

2. If the module **com_absolute_agent_1_1_XXXXX** where _XXXXX_ corresponds to the device configuration appears in the list of modules, then the Agent is installed on the device.

3. If the Agent is installed on the device, confirm whether Customer Center reports the device. If the device does not appear in Customer Center within 30 minutes after installing the Mobile Agent, contact Absolute Software Global Support.

                                    OR

    If the Agent is **not** installed, then continue the troubleshooting process outlined below.

Inspecting Launcher Code Modules

Ensure that the Launcher is fully installed.

To inspect Launcher code modules:

1. On the BlackBerry device, navigate to the list of modules for the Mobile Agent. See _"Required Permissions" on page 29_ for more information on accessing the list of modules.

2. Ensure that the following four modules exist:

    -   com_absolute_launcher_1_2

    -   com_absolute_esn

    -   com_absolute_ws_1_2

    -   com_absolute_apputils_1_2

3. If modules are missing from the device, reinstall the Mobile Agent using the Mobile Agent Bundle for BlackBerry devices.

Confirming Launcher Permissions

The Mobile Agent require the permissions specified in <u>"Required Permissions"</u> <u>on page 29</u>.

NOTE Confirming launcher permissions is only necessary in case BES is not used to install the Mobile Agent. When BES is used to install the Mobile Agent, BES automatically sets the required permissions.

To confirm Launcher permissions:

1. On the BlackBerry device, click the **Applications** icon on the Desktop, then click **Options**, then click **Advanced Options**, and then click **Applications**.

2. Select **Computrace Mobile Launcher**.

                                        OR

   Select **Computrace Mobile Launcher and Dashboard**.

3. Press the **Menu** button, and then click **Edit Permissions**. Ensure that the permissions match those outlined in permissions to match <u>BlackBerry Application Permissions for the Mobile Agent</u>.

Verifying Data Connections

The Launcher requires an active data connection using your mobile network operator to download the Mobile Agent.

NOTE The Launcher uses the data connection that your network operator provides to remain device agnostic. That is, the Launcher application functions on any supported BlackBerry device regardless of device features. The Mobile Agent can contact the Absolute Monitoring Center using a wireless LAN. Not all BlackBerry devices offer features to access wireless LANs.

To access the Internet, BlackBerry devices operating on a GSM network activated using BlackBerry Desktop Software require setting TCP Access Point Name (APN) information.

NOTE BlackBerry devices operating on a CDMA network do **not** require setting TCP APN information to access the Internet. CDMA network operators include Verizon, Sprint, Telus and Bell.

To verify TCP APN settings for a BlackBerry device:

1. On the BlackBerry device, click the **Applications** icon on the Desktop, then click **Options**, then click **Advanced Options**, and then click **TCP**.

2. Ensure that settings are correct for the network operator providing the Subscriber Identity Module (SIM) card in the device.

NOTE See _"Access Point Name Settings" on page 34_ for a list of TCP APN settings for common North American GSM network operators.

Data traffic from BlackBerry devices activated using BlackBerry Enterprise Server routes through the BlackBerry Enterprise Server on which a device was activated. If the Launcher installs on a BlackBerry device activated using BlackBerry Enterprise Server and the Mobile Agent does not download, ensure that the BlackBerry Enterprise Server can communicate with the following Internet addresses:

- https://ctm.server.absolute.com

- http://ctm.agent.absolute.com

To verify that a BlackBerry Enterprise Server can communicate with ctm.server.absolute.com:

1. On the server hosting BlackBerry Enterprise Server, click **Start**, then click **Run**, then type **cmd**, and then click **OK**.

2. At the prompt in the Command window, type **tracert ctm.server.absolute.com**, and then press ENTER

To verify that a BlackBerry Enterprise Server can communicate with ctm.agent.absolute.com:

1. On the server hosting BlackBerry Enterprise Server, click **Start**, then click **Run**, then type **cmd**, and then click **OK**.

2. At the prompt in the Command window, type **tracert ctm.agent.absolute.com**, and then press ENTER

If the trace does not complete, you must configure your network to allow the BlackBerry Enterprise Server to contact https://ctm.server.absolute.com and http://ctm.agent.absolute.com.

Performing a Reset

To perform a reset on a BlackBerry device:

1. Reset your device. Refer to the BlackBerry user guide for your device for instructions on resetting the device.

2. Wait 10 minutes. If the Launcher does not download the Mobile Agent, repeat step 1.

If the Launcher does not download the Agent when you perform a reset on the device, contact Absolute Software Global Support. Be prepared to provide the event log on the device.

To examine the event log on a BlackBerry device:

1. Turn on the BlackBerry device.

2. Press and hold the ALT key, and then press **LGLG**.

Review the event log for any messages referring to modules having a name beginning with the text com_absolute.

See ["Contacting Global Support" on page 2](#) for information on contacting Absolute Software Global Support.

Access Point Name Settings

This section lists Access Point Name (APN) settings for various North American GSM network operators.

Rogers

APN: internet.com

Username: wapuser1

Password: wap

T-Mobile

APN: wap.voicestream.com

Username: (leave blank)

Password: (leave blank)

AT&T

APN: isp.cingular

Username: (leave blank)

Password: (leave blank)

OR

APN: proxy

Username: (leave blank)

Password: (leave blank)

Chapter 8   # Installing Computrace Mobile on S60 Handsets

This chapter provides instructions for using the Nokia PC Suite to install Computrace Mobile for S60 on a handset running S60. The Computrace Mobile for S60 installation process consists of the following parts:

- Installing the S60 Mobile Agent
- Installing the S60 Subscription
- Installing the S60 Dashboard

Supported Devices

Computrace Mobile for S60 supports all models of handsets that use the S60 3rd edition and later releases, such as FP1, FP2, and the 5th edition.

Software Components of Computrace Mobile for S60

Computrace Mobile for S60 contains the following two components:

- The **S60 Agent application** (the Agent) makes data calls to the Absolute Monitoring Centers over TCP/IP. It silently undertakes the functions of the Computrace Mobile for S60 product, such as the collection of Asset or Location data. All data exchanged with the server is encrypted using Secure Sockets Layer (SSL).

- The **Dashboard application** displays the status of the Agent to the user. It provides a menu option to initiate a call to the Absolute Monitoring Center. Access to the Dashboard is password protected by a user selected password. Installation of the Dashboard is optional and the Agent can function normally without it.

Before Installing Computrace Mobile for S60

Before starting the installation of the Computrace Mobile for S60 product, complete the following:

IMPORTANT Ensure that your mobile handset supports S60 3rd edition or later releases.

1. Back up the data on your handset. Refer to the *Instruction Manual for your handset* for the correct process to follow.

2. Download the Computrace Mobile for S60 installation package **CTM-S60-XX-YY.zip** from the **Download Packages** page on Customer

Center. See the *Downloading the Agent* section in the *Customer Center User's Guide* for more information.

3. Extract the contents of Computrace Mobile for S60 installation package **CTM-S60-XX-YY.zip** to a temporary folder on your computer. The temporary folder can be located anywhere on your computer. The package includes the following files:

   ○ Computrace_Agent_S60_*XXXX*.sis

   ○ Computrace_Dashboard_S60_*XXXX*.sis

   > **NOTE** The XXXX characters in the .sis filename stand for the version number of the application. The actual file name might contain a combination of four digits such as 3017 or 3018.

   ○ CTMS60-Subscription.txt

   ○ CTMS60-UninstallKey.txt

   > **IMPORTANT** Note the location of the CTMS60-UninstallKey.txt file. You cannot uninstall the S60 Mobile Agent from your handset without the CTMS60-UninstallKey.txt file. If you cannot locate the file during uninstallation, you can get another copy of the file by downloading the Computrace Mobile for S60 installation package **CTM-S60-XX-YY.zip** again.

   ○ ReleaseNotes.txt

4. Install the latest version of the Nokia PC Suite software compatible with your handset on your computer. You can download the software from the following link: http://www.nokia.co.uk/get-support-and-software/download-software/main/download.

5. Use a suitable tethering mechanism, such as a USB cable, Bluetooth adapter, or Infrared Data Association (IrDA), in combination with the Nokia PC Suite software to connect your computer with your S60 handset. Upon successful connection, Nokia PC Suite displays an image of your handset in the Nokia PC Suite User Interface.

Installing the S60 Mobile Agent

To install the S60 Mobile Agent on your handset:

1. In the Nokia PC Suite interface on your computer, click the **File** menu. The File Menu expands to display a variety of options.

2. Click the **Install Applications** option. The Nokia Application Installer screen opens to display two sections:

   ○ **My Computer** section appearing on the left hand side of the screen

○ **My Phone** section appearing on the right hand side of the screen

3. In the **My Computer** section (left side) of the screen, use the browse button to navigate to the location on your computer where you extracted the contents of the Computrace Mobile for S60 installation package. The files in the selected directory appear as a list in the **My Computer** section of the screen.

4. In the list of files, click **Computrace_Agent_S60_XXXX.sis**. The bottom of the screen refreshes to show information about the selected application and a set of buttons are activated in the middle of the screen.

5. Click the **arrow** button in the middle of the screen. A Nokia Application Installer message dialog opens asking you to continue installation on the mobile handset interface.

6. When prompted on your mobile handset, select **Yes** to install the Agent on your handset. A prompt listing the application name and version number appears.

7. Select **Continue**.

8. If your handset contains a previous installation of the Agent, a confirmation message appears to prompt you to shut down the Agent and replace it with the latest version. When prompted, select **OK** to continue.

9. When a message informing you that the Agent makes periodic data calls that may incur network charges appears, select **OK** to continue. The Agent installer continues installation and displays a confirmation message upon successful completion.

10. Manually copy the **CTMS60-Subscription.txt** subscription file to your handset. See Installing the S60 Subscription for more information.

IMPORTANT If you synchronize your handset following a Data Delete operation, the synchronized data on your computer is also deleted. For example, if a Data Delete command removes a user's contacts, any subsequent sync operation removes these contacts from the PIM provider such as Microsoft Outlook or Lotus Notes. Before executing a Data Delete operation on your handset, back up all sensitive data that can be accidentally deleted upon any subsequent Nokia PC Suite Sync operations.

Installing the S60 Subscription

The S60 Mobile Agent uses the information available in a subscription file to identify the appropriate Customer Center account for your device. You need to copy the subscription file into your handset manually.

To copy the subscription file to your handset:

1. On your computer, browse to the location where you extracted the contents of the Computrace Mobile for S60 installation package.

2. From the list of files, copy the **CTMS60-Subscription.txt** file.

3. In the Nokia PC Suite software interface, open the **File** menu and select **File Manager**. The File Manager screen opens.

4. Browse the folder structure on your handset and open the **Phone Memory\Data\CTM** location. Paste the copied subscription file to the CTM folder on your handset.

    > **IMPORTANT**   If the CTM folder does not exist on your handset, the S60 Mobile Agent installation was not successful. See "Installing the S60 Mobile Agent" on page 36 for information on installing the S60 Mobile Agent on your handset.

On the next call to the Monitoring Center, the Agent processes the subscription file. On successful processing, the subscription file is automatically deleted from your handset.

Installing the S60 Dashboard

To install the S60 Dashboard:

1. In the Nokia PC Suite interface on your computer, click the **File** menu, and select the **Install Applications** option. The Nokia Application Installer screen opens to display two sections:

    ○ **My Computer** section appearing on the left hand side of the screen

    ○ **My Phone** section appearing on the right hand side of the screen

2. In the **My Computer** section, use the browse button to navigate to the location on your computer where you extracted the contents of the Computrace Mobile for S60 installation package. The files in the selected directory appear as a list in the My Computer section of the screen.

3. In the list of files, click **Computrace_Dashboard_S60_XXXX.sis**.

4. Click the **arrow** button in the middle of the screen. A Nokia Application Installer message dialog opens asking you to continue installation on the mobile handset interface.

5. When prompted on your mobile handset, select **Continue** to install the Dashboard on your handset. The installer starts the installation process on your handset. If a newer version of the application is available, the installer displays a prompt asking you to confirm the upgrade.

6. Follow on-screen instructions to continue installation. The installer displays a prompt asking for the location where you want to install the S60 Mobile Dashboard.

7. Provide the desired location details and follow on-screen instructions to continue installation. The Dashboard installer continues installation and displays a confirmation message upon successful completion.

IMPORTANT When working with the Dashboard, make a note of the Dashboard password. You require the password whenever you need to access the Dashboard.

Removing the S60 Dashboard

You can use the in-built Application Manager software to remove the S60 Dashboard directly from the handset.

To remove the S60 Dashboard:

IMPORTANT Before uninstalling the S60 Dashboard, make a note of the Dashboard password. If you need to reinstall the Dashboard at a later date, the password is required to access the Dashboard.

1. On your handset, open the **Application Manager**, also known as **App. manager**, software.

   The location of the Application Manager software varies across different S60 handsets; however, the two common locations for the software are:

   ○ From the standby screen, select **Menu**, then select **Installations**, and then select **App mgr**.

   OR

   ○ From the standby screen, select **Menu**, then select **Settings**, then select **Application Manager**, and then finally select **Installed apps**.

   NOTE If you cannot find the Application Manager software at either of these two locations, refer to the Instruction Manual for your handset for more information.

2. In the Application Manager software interface, select **Computrace Dashboard**.

3. Select **Options**.

4. Select **Remove**. A message confirming that you want to remove the Dashboard displays.

5. Select **Yes**. The Application Manager software uninstalls the Dashboard and displays a confirmation message upon successful removal.

Removing the S60 Mobile Agent

To remove the S60 Mobile Agent from your handset, you need to copy the CTMS60-UninstallKey.txt file containing an uninstallation key to your handset. The text file is available in Computrace Mobile for S60 installation package.

To remove the S60 Mobile Agent from your handset:

1. Copy the file **CTMS60-UninstallKey.txt** from the Computrace Mobile for S60 installation package on your computer to the **Phone Memory\Data\CTM** location on your handset. The copy process is similar to the process followed to copy the subscription file. See "Installing the S60 Subscription" on page 37 for more information.

    IMPORTANT   If the CTM folder does not exist on your handset, the S60 Mobile Agent installation was not successful. See "Installing the S60 Mobile Agent" on page 36 for information on installing the S60 Mobile Agent on your handset.

2. Open the Application Manager software on your handset. See step 1 in the Removing the S60 Dashboard section for details on how to open the Application Manager software.

3. In the Application Manager software interface, select **Computrace Agent**.

4. Select **Options**. The options dialog opens.

5. Select **Remove**. After a short delay, Application Manager displays a prompt to confirm that you want to remove the S60 Mobile Agent.

6. Select **Yes**. Application Manager displays a prompt to confirm shutdown of the S60 Mobile Agent before removing it.

7. Select **OK**. The Agent checks the CTMS60-UninstallKey.txt file to validate the uninstallation key. Upon successful validation, the Application Manager removes the S60 Mobile Agent from your handset and displays a message confirming the removal.

    IMPORTANT   If the CTMS60-UninstallKey.txt fails validation, Application Manager displays two error messages. If validation errors occur, repeat the entire uninstallation procedure from step 1. If you are still unable to remove the S60 Mobile Agent, contact Absolute Technical Support for assistance. See "Contacting Global Support" on page 2 for more information.

Chapter 9   *Installing the Agent on Android Mobile Devices*

This chapter provides instructions for installing the Mobile Agent on devices running the Android operating system.

IMPORTANT Before you begin installation, you need to change your device's settings to allow installation of applications outside the Android Market. To allow outside applications on your device, open the Settings menu of your device, click **Applications**, and then select the **Unknown sources** option.

Supported Operating Systems and Devices

The Mobile Agent for Android devices supports all makes and models of devices running Android OS version 1.5 and later releases.

Downloading and Installing the Mobile Agent

The links to download the Mobile Agent installer for Android devices are available on the **Download Packages** page in Customer Center. The CTMobile.apk file, also known as the CTMobile Installer, installs some or all of the following components depending on the version of the package you downloaded:

- **CTMobileSentinel** (Mandatory)— The Mobile Sentinel application. The Sentinel application ensures that the CTMobile Agent is running at all times.

- **CTMobile Agent** (Mandatory) — the Mobile Agent

- **CTMobileDashboard** (Optional) — the Mobile Dashboard application providing details about the status of the Agent and error logs

To install the Mobile Agent:

1. Log in to Customer Center. The Home Page appears.

2. Click the **Download Packages** link at the bottom of the Home Page.

3. On the **Download Packages** page, click the **Android** link in the **Agent Type** column of the **Agent** table. When prompted, click **Open** or **OK**. The browser displays the download links and instructions.

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

4. The following options are available to download the installation package:

      ○ **Agent Only** — installs the Mobile Agent without the CTMobile Dashboard.

      ○ **Agent with Dashboard** — installs the Mobile Agent along with the CTMobile Dashboard.

If you do not want to distribute the links within your organization, you can use the following links instead:

      ○ **Agent Only** — installs the Mobile Agent without the CTMobile Dashboard. (Install Key and Pass Phase required)

      ○ **Agent with Dashboard** — installs the Mobile Agent along with the CTMobile Dashboard. (Install Key and Pass Phase required)

5. Click one of the e-mail icons to send a link to an appropriate device.

6. On the mobile device, open the e-mail containing the link.

7. Tap on the link. The built-in browser starts automatically.

8. In the browser window, click **Download**. The download starts automatically. When the download is complete, you can see the package listed in the Downloads page of the browser.

> **NOTE** If the download does not start automatically, click the link at the bottom of the page to force the download.

9. On the Downloads page of the browser, tap on **CTMobile.apk** to start the installation of the CTMobile Installer application.

10. When prompted, click **Install**. The CTMobile Installer application is installed and you are presented with a screen confirming that the CTMobile Installer installation is complete.

11. Click **Open** to open the CTMobile Installer. You see a list of following actions that the Installer performs to complete the installation:

      ○ **Install CTMobile Sentinel**

      ○ **Install CTMobile Agent**

      ○ **Install CTMobile Dashboard** (if your CTMobile Installer includes the CTMobile Dashboard)

      ○ **Uninstall CTMobile Installer**

12. Click **Install Applications**. A screen prompting you to install the CTMobile Sentinel opens.

13. Click **Install** to start installing the Sentinel application. When the installation is complete, a confirmation screen opens.

14. Click **Done** to open a screen prompting you to install the CTMobile Agent.

15. Click **Install** to start installing the Mobile Agent. When the installation is complete, a confirmation screen opens.

16. Click **Done**.

17. One of the following happens:

○ If your device is running Android OS 2.2 or higher, a screen prompting you to activate the device administrator and security policies opens. Click **Activate** and continue to step 18.

○ If your device is running Android 2.1 or lower, continue to step 18.

18. If your installer includes the CTMobile Dashboard, a screen prompting you to install the CTMobile Dashboard opens. Click **Install** to install the CTMobile Dashboard.

19. When prompted, click **Done** on the confirmation screen, and then continue to step 20.

20. A screen confirming that the installation process is now complete and that you can now uninstall the CTMobile Installer opens. Click **OK** to open a screen that lets you uninstall the CTMobile Installer.

21. Click **OK** when prompted to uninstall the CTMobile Installer. When the uninstall process is complete, a confirmation screen opens.

22. Click **OK** to close the screen. The selected applications are now installed on your device and the appropriate icons are now available on the Launcher pane of your device. See "Using the CTMobile Dashboard" on page 44 and "Using the CTMobile Dashboard" on page 44 for more information.

> **IMPORTANT** If the version of the installer you downloaded does not include the CTMobile Dashboard, you do not see an icon for the CTMobile Dashboard. If you want to install the CTMobile Dashboard on your device, you need to download the appropriate version and follow the installation process again.

Using the CTMobile Dashboard

After you install the CTMobile Dashboard application, you can use the application to verify that the Mobile Agent is running, view the current status of the Mobile Agent, and place test calls.

Setting Your Password

The first time you run the CTMobile Dashboard, you are prompted to enter a password. The password must be at least eight (8) characters long.

To set your password:

1. On the Launcher pane, click the **CTMobile Dashboard** app.

2. In the **Choose a new password** field, enter a new password. The password must be at least eight (8) characters long.

3. In the **Confirm new password** field, enter the password you entered in step 2.

4. Click **Set Password**. The new password is saved and the home screen opens.

Viewing Agent Status Information

The Agent Status tab in the CTMobile Dashboard provides the following information about the Agent:

- **Agent Status** — the status of the Agent installed on the device. Possible values are:

  - **Idle** — The agent is idle, awaiting the next scheduled call-in time.

  - **Idle - No Connectivity** — There is currently no wifi or data connection available on the device. The agent will not attempt to call in while in this mode.

  - **Activating** — The agent is activating itself with the Monitoring Center. This happens at the beginning of the first ever call.

  - **Initiating Session** — The Agent has initiated a call to the Monitoring Center. This status shows at the start of every call.

  - **Getting Commands** — Receiving the list of commands to be processed for one of the Data and Device Security features. You may see many different instances of the status, one for each feature that is being processed.

  - **Processing Command** — The Agent is processing a command within a feature. For example, processing a Data Delete command for files and folders on the device.

  - **Ending Session** — The Agent is terminating the current call with the Monitoring Center.

- **Identifier** — the unique identifying number of the device

- **Next Call Time** — date and time of next scheduled call from device

- **Last Call Time** — date and time of last call from device

- **Last Call Status** — the status of the last call to the Monitoring Center, possible values are:

  - **Completed Successfully** - The last call to the Monitoring Center completed successfully.

  - **Activation Error** - An error occurred while the agent was activating itself with the Monitoring Center.

  - **Authentication Error** - An error occurred while the agent was "Initiating Session" during the last call.

  - **Session Expired or Invalid** - The Agent is calling into Monitoring Center while another call is active.

  - **Service Error** - General communication failure, not covered by above failures.

       ○   **Call Failed** - General failure, not covered by above communication failures.

- **Agent Version** — the version number of the Mobile Agent installed on the device

- **Monitoring Center** — the server where the Agent calls into

- **Location Tracking** — whether Geo Location tracking is enabled and the number of location samples collected since the last Agent call

To view Agent Status information:

1. On the Launcher pane, click the **CTMobile Dashboard** app.

2. When prompted, enter your password and click **Login** to open the home page of the CTMobile Dashboard.

3. Click the **Agent Status** tab to open the Agent Status page.

Viewing the Agent Log

The Agent Log tab in the CTMobile Dashboard provides a list of errors, if any, encountered by the Agent since the last Agent call to the Monitoring Center. If the location tracking feature reports any errors outside of an Agent call, these errors are also available in the Agent Log.

To view the Agent Log:

1. On the Launcher pane, click the **CTMobile Dashboard** app.

2. When prompted, enter your password and click **OK** to open the home page of the CTMobile Dashboard.

3. Click the **Agent Log** tab to open the Agent Log page.

4. If you would like to view updated Agent Call information, click **Refresh** to refresh the Agent Log page and view updated information.

Placing a Test Call

To place a test call:

1. On the Launcher pane, click the **CTMobile Dashboard** app.

2. When prompted, enter your password and click **OK** to open the home page of the CTMobile Dashboard.

3. Click the **Agent Status** tab to open the Agent Status page.

4. Click **Call In**. If the device is connected to the Internet using Wi-Fi or a data connection, the Android device calls the Monitoring Center.

Changing Your Password

To change your password:

1. On the Launcher pane, click the **CTMobile Dashboard** app.

2. When prompted, enter your password and click **OK** to open the home page of the CTMobile Dashboard.

3. Click the **Agent Status** tab to open the Agent Status page.

4. Click **Change Password**.

5. When prompted, enter the existing password, the new password, and confirm the new password in the appropriate fields.

6. Click **Update Password**. The new password is saved.

Troubleshooting Problems With the Mobile Agent

If you are experiencing problems with the Mobile Agent, you can send detailed diagnostic information about these problems using the CTMobile Dashboard to Absolute Software.

To send diagnostic information:

1. On the Launcher pane, click the **CTMobile Dashboard** app.

2. When prompted, enter your password and click **OK** to open the home page of the CTMobile Dashboard.

3. Click the **Agent Log** tab to open the Agent Log page.

4. Press the **Menu** button on your device to show additional buttons on the Agent Log page.

5. Click **Send Log. One of the following happens:**

    ○ If you have set up only one mailbox on your device, the e-mail app opens. The Compose e-mail window opens. Continue to step 6.

    ○ If you have set up more than one e-mail account on your device, the Choose e-mail application dialog box opens. Click the appropriate application name to select the e-mail application that you want to use to send the e-mail. We recommend that you use Gmail. The Compose e-mail window opens. Continue to step 6.

6. If you want to change the default e-mail address, enter the new e-mail address in the **To** field. The default e-mail address where the diagnostic information is sent is **support@absolute.com**.

    You can also add another e-mail address in addition to the default e-mail address. Separate different e-mail addresses with commas.

7. If you want to change the subject of the e-mail, enter the new subject in the **Subject** field.

8. Click **Send**. The e-mail is sent to the e-mail addresses specified in the first field.

Deploying the Agent Using Systems Management Server

The purpose of this document is to provide instructions on setting up a deployment package and deploying the Agent to a group of machines on a network using **Microsoft Systems Management Server (SMS)**.

The instructions in this document are specific to **SMS 2003 SP3** running on **Windows 2003 Server SP2** and **SQL Server 2000 SP4**. Setup and installation procedures for previous versions of SMS or for **Microsoft System Center Configuration Manager 2007** may vary somewhat from the procedures documented below.

IMPORTANT The instructions provided in this document represent generic guidelines only. You may need to make minor changes to the procedural steps below to reflect your specific network configuration.

Deployment Prerequisites

In order to set up and deploy the Agent using SMS, you need the following:

- **SMS Server** must be installed.
- The **SMS Server** must be a member server in an **Active Directory** domain.
- The Agent installer (**Computrace.exe**) for your company must be available. It should reside on the closest file server to your SMS distribution point.
- **Internet Information Server (IIS)** must be installed on your **SMS Server** (for reporting).
- You must have administrative privileges on your network.

NOTE If you are storing the **Computrace.exe** installer on a public file server, be sure to create a private share folder for the installer. To create a private share, add a dollar sign ($) to the end of your share name (e.g. **ComputraceInstall$**).

To deploy software across a network using SMS, you first create a package containing the software you wish to deploy, and then advertise the availability of the package on your network. When a client machine logs in, it receives the advertisement, and the software is automatically installed on the client machine.

Network partitioning with SMS is similar to Windows Active Directory - your network is partitioned into different sites. When you build the SMS package and advertisement, you must make sure that all intended sites get the package, otherwise not all computers in your network receive the installation package.

Deployment Procedure

To create a package and deploy the Agent to your network using SMS:

1. Copy **Computrace.exe** to your SMS distribution point.

2. Login to the SMS server. Click **Start > All Programs > Systems Management Server > SMS Administrator Console**. The **SMS Administrator** console opens, displaying the site database.

3. In the left navigation pane, double-click to expand the **Systems Management Server** site database.

4. Navigate to the **Package** entry and right-click.

5. From the popup menu, select **New > Package From Definition**. The **Create Package From Definition Wizard** appears.

6. Click **Next**.

7. Browse to the location of the **Computrace.exe** file (located on your distribution point/file share).

8. Select **Computrace.exe** and click **Open**. The **Publisher** field is populated with the value **Absolute Software Inc**. The package definition lists additional attributes of the installer.

9. Click **Next**. The **Source Files** window appears.

10. Select **Always obtain files from a source directory**, then click **Next** (unless you have an alternate setup location).

11. The **Source Directory** window appears. Select the location of your **Computrace.exe** file. Click **Next**.

12. The summary window appears. Click **Finish**. The package is created and displayed in the list on the right pane.

> **IMPORTANT** Be sure to make a note of the package ID.

13. Right-click on **Packages** in the left navigation window and select **All Tasks > Distribute Software**. The **Distribute Software** wizard appears.

14. Click **Next**. The **Package** window appears.

15. Select the package you have just created and click **Next**.

16. The **Distribution Points** window appears. Click on **Select All** (especially if you have multiple SMS distribution points).

17. Click **Next**. The **Advertise a Program** window appears. Click **Yes** to advertise the package, then click **Next**.

18. The **Select a Program To Advertise** window appears. The **Package** lists **Computrace**. Select the **Per-system unattended** option, then click **Next**.

19. The **Advertisement Target** window appears. Click on the **Create a new collection and advertise this program to it** radio button, then click **Next**.

20. The **New Collection** window appears. Enter the **Name** for the new collection, and a comment if desired, then click **Next**.

21. The **Collection Membership Rules** window appears. This determines which users receive the package. Your company's membership group(s) should already be set up and available for selection. Select the membership group and click on **Next**.

> **NOTE** You can click on the **Schedule** button and, if desired, modify the scheduling of the distribution. Generally, however, you can just accept the default schedule, as it likely conforms to the schedule of your existing software deployments.

22. The **Advertisement Name** window appears, listing the name of the package based on your previous entries. Add a comment if desired and click **Next**.

23. The **Advertise to Subcollections** window appears. Click on the **Advertise the program to members of subcollections as well** (default value). Click **Next**.

24. The **Advertisement Schedule** window appears. The default settings display the current time and date. Choose whether or not to expire the advertisement:

     ○ **No. This advertisement never expires** (default)

     ○ **Yes. This advertisement should expire** (Select expiry date and time).

     Click **Next**.

25. The **Assign Program** window appears. Click **Yes** and assign the program to the immediate date and time. Click **Next**.

> **NOTE** In general, you can accept the default date and time and expiration criteria for your advertisement, unless you want to change the initial installation time, or you want your advertisement to expire on a specific date and time.

26. The **Summary** window appears. Click **Finish**.

27. Click on the **Advertisements** entry in the left navigation window to see the newly created **Advertisement**.

SMS begins deploying the Agent installer to all selected machines.

Monitoring Your Deployment

To view the status of your package:

➢ On the left navigation pane, navigate to **System Status > Package Status** then select your package name.

To view the status of your advertisement:

➢ On the left navigation pane, navigate to **System Status > Advertisement Status**, then select your advertisement name.

The status of your advertisement indicates how many machines have received the deployment, and whether any errors have occurred.

Running Reports

The SMS all packages report gives you an overview of the Agent Installer package and any other SMS packages on your server. To run the SMS All Packages report:

➢ Go to the **SMS Reporting** Web site and run the **All Packages** report.

NOTE You can also run this report from the **Reporting** entry on the left navigation menu of the **SMS Administrator Console**. Make sure **Internet Information Server (IIS)** is installed prior to running the report.

Debugging Your Deployment

If you experience difficulties with your SMS deployment, check for the following potential problems:

- If no machines are getting the installation package, check your network permissions.
- If only some of the machines are getting the package, check your package definition to ensure that all sites which should receive the package are included.

Re-running the Advertisement

If you need to re-run your advertisement:

1. Navigate to the **Advertisements** entry in the left navigation menu.
2. Right-click on your advertisement.
3. From the pop-up menu, select **All Tasks > Re-run Advertisement**.

Chapter 11 *Deploying the Agent Using an Active Directory Script*

The **Computrace.exe** installation file conforms to industry standards for MSI files, enabling network administrators to deploy the Agent into their environment using Active Directory.

This chapter provides sample instructions for deploying the Agent using a startup script in Active Directory. These instructions are generic and intended to serve as a starting point for developing your own scripts.

> **NOTE** For the remainder of this chapter, a basic understanding of Active Directory structure and terminology is assumed. An organizational unit (OU) or container is a subdivision within an Active Directory where you can place users, groups, computers, and other organizational units.

Using the example below, the following instructions would deploy the Agent on all machines located in the OU=Computer, OU=Vancouver, OU=BC Active Directory domain. Additionally, the installation would occur once per computer as opposed to once per user. When performing an Active Directory deployment at your site, replace the values listed in the example below with your own settings.

1. Open **Active Directory Users and Computers**

2. If necessary, build the tree structure you require. For example:

   - OU=BC

   - OU=Vancouver,OU=BC

   - OU=Computers,OU=Vancouver,OU=BC

   - OU=Users,OU=Vancouver,OU=BC

3. Right-click the **OU=Computers,OU=Vancouver,OU=BC** container and select **Properties**.

4. Click the **Group Policy** tab and click **New**. Define a name for the new policy.

5. Right-click the new policy and select **Properties**, click the **Security** tab and grant **Full Control** to the **System** group. Click the **OK** button.

6. View the **Group Policy Object Links** for the policy.

7. Browse to **Computer Configuration > Windows Settings > Scripts** and view the properties of the **Startup** script.

8. Click the **Add** button and add the **Computrace.exe** program with the `-sp/s` switch as in this example:

   ```
   Computrace.exe -sp/s
   ```

   The `-sp` switch is used to pass Install Shield command line arguments to the installer. The /s switch performs a silent install. Installation occurs in the background.

9. Copy the Agent setup files to the Active Directory scripts folder:
   ```
   c:\windows\sysvol\domain\policies\%PolicyNumber%\Mach
   ine\Scripts\startup
   ```

   NOTE The specific path can be viewed by clicking the **Show Files** button in the Startup Properties.

10. Test the script.

    IMPORTANT Absolute Software recommends testing your script on a single PC before deploying across your environment.

Table 1.

Installation Stage	Item	Description	✓
Installation — Non-BIOS PCs	Set boot order to *Boot Order HDD 1st, FDD\CDROM.*	Change the device boot order to Hard Drive (HDD) first. Changing the boot order is not necessary on devices with BIOS based persistence.	☐
Installation — BIOS PCs	Set BIOS Administrator password.	Set a BIOS password to gain additional security and prevent unauthorized access to the BIOS.	☐
Installation —Script or Manual Install	Remove the Agent installer from the device after completing installation.	Be careful when removing the local copy of the Agent installer after completing installation.	☐
Installation — Image Install	Incorporate the Agent installer into the disk image.	Incorporate the Agent installer into any images used for repair or maintenance.	☐
Installation — Activation	Confirm that each Identifier is uniquely activated.	Once the Agent is installed on a device, confirm that the Agent has contacted the Monitoring Center and acquired a unique Identifier. As the physical serial number of the device is directly associated to its electronic counterpart, ensuring its uniqueness is critical.	☐
Maintenance — O/S Reinstall	Reinstall the Agent.	When removing and installing an operating system, even if it is the same operating system, reinstall the Agent. On devices with BIOS based persistence the Agent is reinstalled automatically.	☐
Maintenance — Hard Drive Replacement	Reinstall the Agent.	Ensure that the Agent is reinstalled in cases where hard drives have been replaced. This will occur automatically with BIOS based persistence	☐
Maintenance — System board Replacement	Update the serial number in the BIOS (DMI information) of the device.	Work with your vendor to ensure that the new system board contains the physical serial number shown on the device.	☐

Table 1.

Installation Stage	Item	Description	✓
Monitoring/ Drift	Monitor when machines 'drift' or have not called in for more than 30 days.	Proactively identify any devices that have not contacted the Monitoring Center for an unusually long period of time (Greater than 30 days).	☐
License Management	Retire the Identifier associated with a retired or destroyed device.	Retired (or disabled) Identifiers no longer consume a license, and do not appear in Customer Center reports unless specifically selected.	☐

Appendix B *BlackBerry Application Permissions for the Mobile Agent*

Item	Permission
Connections	**Custom**
USB	Allow
Bluetooth	Allow
Phone	Allow
Location (GPS)	Allow
Server Network or Company Network	Prompt
Internet or Carrier Internet	Allow
Interactions	**Custom**
Cross Application Communication or Interprocess Communication	Allow
Device Settings	Allow
Media	Allow
Application Management or Module Management	Allow
Keystroke Injection	Deny
Browser Filters	Deny
Themes or Themes Data	Allow
Security Timer Reset	Deny
User Data	**Allow**
Email/Messaging	Allow
Organizer Data or PIM	Allow
Files	Allow
Security Data	Allow
Key Store	Allow
Key Store Medium Security	Allow

Index