Copyright

Copyright 2018 Webroot. All rights reserved.

WSA Management Website User Guide

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Webroot.
# Table of Contents

Chapter 1: WSA Management Website User Guide ................................................. 1  
Webroot SecureAnywhere Management Website User Guide Overview .................. 2  

Chapter 2: Getting Started ................................................................................. 4  
System Requirements for Management Website ................................................. 5  
  System Requirements for Android Devices ...................................................... 5  
  System Requirements for iOS Devices ............................................................. 5  
  System Requirements for Windows .................................................................. 5  
  System Requirements for Mac ......................................................................... 6  
Operating System ............................................................................................... 6  
Creating Accounts .............................................................................................. 8  
Logging In to Your Account ............................................................................... 16  

Chapter 3: Managing Your Account ................................................................. 19  
Adding Devices With Different Keycodes ......................................................... 20  
Managing Consoles ............................................................................................ 23  
  Changing Default Console Names .................................................................. 23  
  Adding Consoles ......................................................................................... 24  
Switching Between Consoles ............................................................................ 27  
Adding Users ..................................................................................................... 29  
Editing Account Settings .................................................................................. 34  
  Adding Your Name, Phone Number, or Time Zone ........................................ 35  
  Changing Your Password ............................................................................. 37  
  Changing Your Security Code ...................................................................... 38  
  Changing Your Security Question ................................................................. 39  

Chapter 4: Using PC Security ........................................................................... 41  
Viewing PC Statuses .......................................................................................... 42  
Adding PCs ........................................................................................................ 45  
Editing PC Security Settings ............................................................................. 48  
Viewing PC Scan Information ............................................................................ 53  
Scanning PCs Remotely ..................................................................................... 59  
Running System Optimizer Remotely ............................................................... 65  
Deactivating PCs ............................................................................................... 71  
Locking, Shutting, Down, or Restarting PCs ..................................................... 78  

Chapter 5: Using Mobile Security ................................................................. 84  
Adding Mobile Devices ...................................................................................... 85
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Mobile Account Information</td>
<td>86</td>
</tr>
<tr>
<td>Viewing Mobile Security Statuses and Alerts</td>
<td>88</td>
</tr>
<tr>
<td>Viewing Mobile Histories</td>
<td>90</td>
</tr>
<tr>
<td>Using Lost Device Protection Commands</td>
<td>92</td>
</tr>
<tr>
<td>Changing Phone Numbers</td>
<td>96</td>
</tr>
<tr>
<td>Removing Mobile Devices</td>
<td>98</td>
</tr>
<tr>
<td><strong>Chapter 6: Using Backup And Sync</strong></td>
<td>100</td>
</tr>
<tr>
<td>Backup &amp; Sync Overview</td>
<td>101</td>
</tr>
<tr>
<td>Storing Files in the Anywhere Folder or in Your Own Sync Folders</td>
<td>101</td>
</tr>
<tr>
<td>Backing Up Files</td>
<td>102</td>
</tr>
<tr>
<td>Getting Started With Backup &amp; Sync</td>
<td>103</td>
</tr>
<tr>
<td>Managing Files and Folders</td>
<td>105</td>
</tr>
<tr>
<td>Renaming Files</td>
<td>105</td>
</tr>
<tr>
<td>Moving Files</td>
<td>106</td>
</tr>
<tr>
<td>Deleting Files or Folders</td>
<td>107</td>
</tr>
<tr>
<td>Creating Folders</td>
<td>108</td>
</tr>
<tr>
<td>Customizing Displays</td>
<td>110</td>
</tr>
<tr>
<td>Switching Views</td>
<td>110</td>
</tr>
<tr>
<td>Customizing Folder Displays</td>
<td>111</td>
</tr>
<tr>
<td>Refreshing Data</td>
<td>111</td>
</tr>
<tr>
<td>Restoring Files From the Recycle Bin</td>
<td>113</td>
</tr>
<tr>
<td>Downloading Files From Your Account</td>
<td>115</td>
</tr>
<tr>
<td>Uploading Files and Folders</td>
<td>117</td>
</tr>
<tr>
<td>Viewing Version Histories</td>
<td>119</td>
</tr>
<tr>
<td>Viewing Device Details</td>
<td>121</td>
</tr>
<tr>
<td>Viewing Activity Logs</td>
<td>124</td>
</tr>
<tr>
<td>Using the Windows Store App for Backup &amp; Sync</td>
<td>126</td>
</tr>
<tr>
<td>Viewing Account Details</td>
<td>129</td>
</tr>
<tr>
<td><strong>Chapter 7: Working With Passwords</strong></td>
<td>131</td>
</tr>
<tr>
<td>Getting Started With Passwords</td>
<td>132</td>
</tr>
<tr>
<td>Using the Password Manager Toolbar</td>
<td>135</td>
</tr>
<tr>
<td>Accessing Passwords From Your Account</td>
<td>142</td>
</tr>
<tr>
<td>Capturing Login Credentials</td>
<td>146</td>
</tr>
<tr>
<td>Capturing Login Credentials While in a Website</td>
<td>146</td>
</tr>
<tr>
<td>Defining Login Credentials From the SecureAnywhere Website</td>
<td>152</td>
</tr>
<tr>
<td>Capturing Additional Login Credentials</td>
<td>155</td>
</tr>
<tr>
<td>Logging in to Password-Managed Sites</td>
<td>160</td>
</tr>
</tbody>
</table>
Chapter 1: WSA Management Website User Guide

To use the Management Website, see the following topic:

Webroot SecureAnywhere Management Website User Guide Overview ........................................ 2
Webroot SecureAnywhere Management Website User Guide Overview

The Webroot SecureAnywhere™ management website provides a central portal from which you can view and manage your protected devices. To access this website, open a browser, go to my.webrootanywhere.com and enter your Webroot account credentials. After you log in, the SecureAnywhere website displays your account data and the security status of all your devices.

The SecureAnywhere management website looks similar to the example below. Depending on the SecureAnywhere edition you purchased, whether it's AntiVirus, Internet Security Plus, or Complete, some panels might be inactive.

The Mobile Security panel is inactive if you did not activate SecureAnywhere protection on a smartphone or tablet.

The Backup & Sync and Passwords panels are inactive if your SecureAnywhere edition does not include those features. For upgrade information, see Webroot's product offerings.

The SecureAnywhere management website provides the following features:
• **PC Security** — Get a global view into all your PCs with SecureAnywhere installed. Using a web browser from a remote location, you can see whether your computers are secure or infected.

  **Note:** Coming soon: Mac Security will be included in the SecureAnywhere management website.

• **Mobile Security** — Get a global view into all your smartphones and tablets with SecureAnywhere installed. If necessary, you can remotely locate a missing mobile device with the Lost Device Protection feature.

• **Backup & Sync** — If your edition includes [Backup & Sync](#), you can access your synchronized and archived files. Using a web browser from a remote location, you can download the latest version of a document from your home or office computer, even if your home or office computer is turned off.

• **Passwords** — If your edition includes the [Passwords](#) feature, you can access your saved passwords and profiles. For example, if you can't remember your banking site login, you can go to the Passwords panel and view your user name and password.

• **Account Administration** — Upgrade your products, and add other devices and users to your account. If you are an administrator who manages device security for others, you can organize groups of devices into consoles. A console can include a view of your home devices or your business devices.
Chapter 2: Getting Started

To get started with Management Website, see the following topics:

- System Requirements for Management Website ................................................................. 5
- System Requirements for Android Devices ........................................................................... 5
- System Requirements for iOS Devices ................................................................................ 5
- System Requirements for Windows ...................................................................................... 5
- System Requirements for Mac ............................................................................................. 6
- Operating System .............................................................................................................. 6
- Creating Accounts ............................................................................................................. 8
- Logging In to Your Account .............................................................................................. 16
System Requirements for Management Website

The following describes the system requirements for using Management Website functionality on Windows and Mac and on Android and iOS devices.

System Requirements for Android Devices

Operating Systems

- Android operating system version 4.4 (Kit Kat) or higher.

Devices

- Android-compatible phones and tablets, including Kindle and Nook.

Note: Requires an active internet connection for some features. For a list of these features, click here.

System Requirements for iOS Devices

Operating Systems

- iOS 10 or later.

Devices

- Compatible with iPhone®, iPod Touch®, and iPad® mobile digital devices.

System Requirements for Windows

Operating Systems

- Windows 10 (32-bit and 64-bit).
- Windows 8 and 8.1 (32-bit and 64-bit).
- Windows 7 (32-bit and 64-bit), Windows 7 SP1 (32-bit and 64-bit).
- Windows Vista® (32-bit), Windows Vista SP1, SP2 (32-bit and 64-bit).
RAM

- Intel Pentium®/Celeron® family, or AMD® K6™/Athlon®/AMD Duron™ family, or other compatible processor.
- 128 MB RAM (minimum).
- 2 GB RAM recommended (minimum).

Hard Disk Space

- 15 MB

Internet/Browser

- Internet access is required.
- Google Chrome® (32-bit and 64-bit); current and previous two versions
- Internet Explorer® (32-bit and 64-bit); version 11
- Microsoft Edge® (32-bit and 64-bit); current and previous two versions
- Mozilla® Firefox® (32-bit and 64-bit); current and previous two versions
- Safari; current and previous two versions
- Opera; current and previous two versions

System Requirements for Mac

Operating System

- Mac OS X 10.7 (Lion®)
- Mac OS X 10.8 (Mountain Lion®)
- OS X 10.9 (Mavericks®)
- OS X 10.10 (Yosemite®)
- OS X 10.11 (El Capitan®)
- macOS 10.12 (Sierra®)
- macOS 10.13 (High Sierra®)
**Memory**

- 128 MB RAM (minimum)

**Storage**

- 15 MB

**Internet/Browser**

- Internet access is required.
- Google Chrome® (32-bit and 64-bit); current and previous two versions
- Internet Explorer® (32-bit and 64-bit); version 11
- Microsoft Edge® (32-bit and 64-bit); current and previous two versions
- Mozilla® Firefox® (32-bit and 64-bit); current and previous two versions
- Safari; current and previous two versions
- Opera; current and previous two versions
Creating Accounts

To use the SecureAnywhere website, you must create a Webroot account as described in this section.

**Note:** When you create an account, you automatically become the account administrator. The administrator has full permissions on all account functions, which include adding other users and specifying permissions for those users.

Before you begin, do the following:

- Install SecureAnywhere on your computer. We recommend that you install SecureAnywhere first, but you can do it later if you want.
- Have available the license keycode you used to install SecureAnywhere. If you have additional products and additional keycodes, you can add them later.
- Make sure you are using one of the following browsers:
  - Internet Explorer® version 11 and newer
  - Microsoft Edge® version 37 and newer
  - Mozilla® Firefox® version 40 and newer
  - Google Chrome® 40 and newer
  - Safari® 8 and newer
  - Opera® 27 and newer

**To create an account:**

2. In the Create an account area, click the **Sign up now** button.

The Create an account window displays.
3. Enter your information in the fields in the Create an account window, using the information in the following table.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webroot Product</td>
<td>Enter the license keycode you received when you purchased the product.</td>
</tr>
<tr>
<td>Keycode</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td>Enter your email address, which will also be used for your login name. Your account activation confirmation will be sent to this address.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a minimum of 9 characters. Your password must contain at least 6 alphabetic characters and 3 numeric characters. Your password can be longer than the required 9 characters. It can include special characters, except for angle brackets: &lt; and &gt;. Your password is case sensitive. As you type, the Strength meter shows how secure your password is. For optimum security, you should make your password as strong as possible.</td>
</tr>
<tr>
<td>Your Personal Security Code</td>
<td>Enter a word or number, which will be used for an extra security step after you enter the password during login. Use a code that is easy to remember, using a minimum of six characters. Every time you log in, you must also enter two random characters of this code. For example, if your code is 123456 and it prompts you for the fourth and sixth character, you would enter 4 and 6. Your Personal Security Code is case sensitive.</td>
</tr>
<tr>
<td>Security Question</td>
<td>Select a question from the drop-down list. If you later forget the details of your login, you need to provide the answer to this question to retrieve the information.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Security Answer</td>
<td>Type an answer to your security question. The Security Answer is case-sensitive.</td>
</tr>
<tr>
<td>Please select your storage region</td>
<td>For Backup &amp; Sync users, specify a region where you want your storage server located.</td>
</tr>
</tbody>
</table>

4. After you enter account details, click the **Register Now** button.

SecureAnywhere displays a confirmation message and sends an email to the address you specified. This may take a few minutes.

**Note:** If your SecureAnywhere edition includes the Backup & Sync feature, another field displays that prompts you to select a storage region. Select the region closest to you, U.S., Europe, or Japan, then click the **Register Now** button again.

5. From your email system, open the confirmation email from Webroot and click the link. Your account will not be created until you click this link.

6. When SecureAnywhere prompts you to enter two characters from the Personal Security Code, type the requested characters and click the **Confirm Registration Now** button.

For example, if your code is 123456 and it prompts you for the fourth and sixth characters, you would enter 4 and 6.
Chapter 2: Getting Started

**Note:** As needed, you can deselect the Use Security Code during log in checkbox so that you or other users do not have to enter a two-digit security code when you log in. For more information, see *Adding Users on page 29* and *Editing Account Settings on page 34*.

The SecureAnywhere website opens, similar to the following example. The options that display depend on which SecureAnywhere editions you purchased, for example, [WSA AntiVirus](#), [WSA Internet Security Plus](#), or [WSA Complete](#).

![SecureAnywhere Website](image)

The SecureAnywhere website provides the following features:
<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PC Security</strong></td>
<td>Get a global view into all your PCs with SecureAnywhere installed. Using a web browser from a remote location, you can see whether your computers are secure or infected.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Mac Security is included in the SecureAnywhere website.</td>
</tr>
<tr>
<td><strong>Mobile Security</strong></td>
<td>Get a global view into all your smartphones and tablets with SecureAnywhere installed. If necessary, you can remotely locate a missing mobile device with the Lost Device Protection feature.</td>
</tr>
<tr>
<td><strong>Backup &amp; Sync</strong></td>
<td>Access your synchronized and archived files, if your SecureAnywhere edition includes Backup &amp; Sync. Using a web browser from a remote location, you can download the latest version of a document from your home or office computer.</td>
</tr>
<tr>
<td></td>
<td>For more information, see GETTING STARTED WITH BACKUP &amp; SYNC on page 103.</td>
</tr>
</tbody>
</table>
## Chapter 2: Getting Started

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Passwords</strong></td>
<td>Access your saved passwords and profiles, if your SecureAnywhere edition includes the <a href="#">Passwords</a> feature. For example, if you can't remember your login to a banking site, you can go to the Passwords panel and view your user name and password. For more information, see <a href="#">Getting Started With Passwords on page 132</a>.</td>
</tr>
<tr>
<td><strong>Account Administration</strong></td>
<td>Upgrade your products, add other devices, and manage additional users in your account. If you are an administrator who manages device security for others, you can organize groups of devices into consoles. A console might include a view of your home devices or your business devices. For more information, see <a href="#">Managing Consoles on page 23</a>.</td>
</tr>
</tbody>
</table>
Logging In to Your Account

To log in to your account in the SecureAnywhere website:

2. In the Log in window, enter the email address and password you specified when you registered.
3. Click the Log in button.

4. At the personal security code prompt, type the requested characters and click the Log in button.

Note: As needed, you can deselect the Use Security Code during log in checkbox so that you or other users do not have to enter a two-digit security code when you log in. For more information, see Adding Users on page 29 and Editing Account Settings on page 34.

This personal security code was defined when you created a Webroot account. Every time you log in, SecureAnywhere will require this extra security step. Be aware that it prompts for two random characters of your code. For example, if your code is 123456 and it prompts you for the fourth and sixth characters, you would enter 4 and 6.

Note: If you forgot your password or security code, click the Can't log in? link, then click I forgot my password or I forgot my security code. SecureAnywhere prompts you to enter your
email address and sends you an email message containing a link for resetting your password or security code.
Chapter 3: Managing Your Account

To manage your account, see the following topics:

- Adding Devices With Different Keycodes ............................................................. 20
- Managing Consoles .................................................................................................. 23
  - Changing Default Console Names ........................................................................ 23
  - Adding Consoles .................................................................................................. 24
  - Switching Between Consoles ............................................................................... 27
- Adding Users ........................................................................................................... 29
- Editing Account Settings ......................................................................................... 34
  - Adding Your Name, Phone Number, or Time Zone ............................................. 35
  - Changing Your Password ...................................................................................... 37
  - Changing Your Security Code .............................................................................. 38
  - Changing Your Security Question ....................................................................... 39

- 19 -
Adding Devices With Different Keycodes

If you installed SecureAnywhere on multiple PCs using the same multi-license keycode, the SecureAnywhere website displays information for these PCs after a scan runs on each one. If you installed another Webroot product on a device that uses a different keycode, you must manually add that keycode to your account, as described in this section.

To add a device to your account:

1. Make sure SecureAnywhere is installed on the device you want to manage.
2. Open your browser to the SecureAnywhere website at my.webrootanywhere.com.
3. In the Log in window, enter the email address and password you specified when you registered.
4. Click the Log in button.

5. If you have multiple consoles, select the console under which you want to add the new keycode.

   For more information, see Managing Consoles on page 23.

6. From the drop-down menu next to your login ID, select Manage Keycodes.
SecureAnywhere displays the keycodes page.

7. Click the **Add Product Keycode** button

![Manage Keycodes](image)

8. In the next panel, enter the new code and click **Add**.

   SecureAnywhere verifies the code.

9. Run a scan on the device.

   When the scan completes, it reports its status to the website.
Managing Consoles

When you first registered an account, SecureAnywhere organized your managed devices into a single console. A console is a collection of one or more devices running a Webroot product. If needed, you can create multiple consoles, which can be convenient if you are managing devices for different people and different purposes.

For example, a small business owner might want to create consoles for home and business. The home console could include the laptops and mobiles devices of family members. The business console could include laptops and mobile devices of employees. By creating these separate consoles, the administrator has simplified views into the devices used by family or by employees.

This topic contains the following procedures:

- Changing Default Console Names
- Adding New Consoles
- Switching Between Consoles

Note: A single console is sufficient for most people.

Changing Default Console Names

After you first create an account, SecureAnywhere automatically organizes your devices into a default console called Unnamed Console. If needed, you can change it to a more meaningful name.

To change the default console name:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.
2. To the right of the console name, click the Rename button.
3. Enter a name for the console, using alphanumeric characters and spaces only.
4. Click the **Save** button.

![](image)

**Adding Consoles**

If you manage multiple devices for friends or employees, you might want to organize them into separate consoles.

**To add a console:**

1. Obtain a new keycode from Webroot for the devices that will be managed in the new console. Install SecureAnywhere on those PCs with that new keycode.
2. Open your browser to the SecureAnywhere website at [my.webrootanywhere.com](http://my.webrootanywhere.com).
3. Instead of logging in to your account, click the **Sign up now** button.
   
   The system displays the same registration page you used to create your account.

4. In the Webroot Product Keycode field, enter the new keycode.
5. In the remaining fields, enter your existing account information for the email address, password, security code, and security question and answer.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Webroot Product Keycode</td>
<td>Enter the license keycode you received when you purchased the product.</td>
</tr>
<tr>
<td>Email Address</td>
<td>Enter your email address, which will also be used for your login name. Your account activation confirmation will be sent to this address.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a minimum of nine characters. Your password must contain at least 6 alphabetic characters and 3 numeric characters. Your password can be longer than the required 9 characters. It can include special characters, except for angle brackets: &lt; and &gt;. Your password is case sensitive. As you type, the Strength meter shows how secure your password is. For optimum security, you should make your password as strong as possible.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Your Personal Security Code</td>
<td>Enter a word or number, which will be used for an extra security step after you enter the password during login. Use a code that is easy to remember, using a minimum of 6 characters. Every time you log in, you must also enter two random characters of this code. For example, if your code is 123456 and it prompts you for the fourth and sixth character, you would enter 4 and 6. Your Personal Security Code is case sensitive.</td>
</tr>
<tr>
<td>Security Question</td>
<td>Select a question from the drop-down list. If you later forget the details of your login, you need to provide the answer to this question to retrieve the information.</td>
</tr>
<tr>
<td>Security Answer</td>
<td>Type an answer to your security question. The Security Answer is case-sensitive.</td>
</tr>
<tr>
<td>Please select your storage region</td>
<td>For Backup &amp; Sync users, specify a region where you want your storage server located.</td>
</tr>
</tbody>
</table>

6. Click the Register Now button.

Because you already created an account using your email address, SecureAnywhere recognizes your information. The system prompts you to create a new console for the device.
7. Click the **Select** button in the left panel to add a new console.

   SecureAnywhere creates the console and prompts you to log in.

8. Log in with your account information.

   A panel similar to the following example displays.

9. Select the new **Unnamed Console**. You can rename it later, as described above.

   ![Console Options](image)

   Your new console shows any device that use the keycode you entered.

**Switching Between Consoles**

To switch between two consoles:
1. Click the **Change console** button.

2. Select the console you want to view.
Adding Users

SecureAnywhere allows you to add other users to your account. You can then give them permission to access security-related information on their devices using your account website.

To add a user:

2. In the Log in window, enter the email address and password you specified when you registered.
3. Click the **Down** arrow at the right of your login ID, then select **Manage Users**.

SecureAnywhere displays a list of users for this account.

4. Click the **Create New Users** button.

The Create New User window displays.
5. In the Email Address field, enter an email address for this user.

6. In the Time Zone field, click the Pencil icon to the right of the field, then type the country, region, or city to display a drop-down menu of choices.

7. If needed, select the **Do you wish to give this user Console access?** checkbox to give this user access to your account.

   When you select the **Do you wish to give this user Console access?** checkbox, additional fields display.
8. From the SecureAnywhere drop-down menu, select one of the following permission levels:
   - **Basic** — Grants limited access to consoles and account settings
   - **Admin** — Grants full access to all keycodes, users, and account settings in Webroot portals.

   SecureAnywhere is the home page of [my.webrootanywhere.com](http://my.webrootanywhere.com). From here, the user can access the other Webroot portals, for example, PC Security, Mobile Security, Backup & Sync.

9. From the PC Security drop-down menu, select one of the following permission levels:
   - **Basic** — Grants read-only access
   - **Admin** — Grants full access.

   PC Security is the portal for viewing scan status on the PCs and sending commands to the PCs. For more information, see *Viewing PC Statuses on page 42*.

10. From the Mobile Security drop-down menu, select one of the following permission levels:
    - **Basic** — Grants read-only access.
    - **Admin** — Grants read-only access.

    Mobile Security is the portal for viewing scan status on the mobile devices and for sending commands to the devices. For more information, see *Adding Mobile Devices on page 85*.

11. From the Backup & Sync drop-down menu, select one of the following permission levels:
    - **Basic** — Grants read-only access.
    - **Admin** — Grants read-only access.

    Backup & Sync is the portal for accessing data stored with the Backup & Sync component. For more information, see *Backup & Sync Overview on page 101*.

12. If needed, select the **Passwords Services?** checkbox to give this user access to the Passwords feature. For more information, see *Getting Started With Passwords on page 132*.

   When you select the **Passwords Services?** checkbox, additional fields display.
   - To enable service for this user, select the **Passwords** checkbox.
   - To associate a keycode with the Password feature, from the **Select a keycode** drop-down menu, select the keycode to associate.
13. When you're done, click the **Create User** button.

Webroot sends a confirmation email with an initial password to the address you specified. The user opens the email, clicks the link, pastes in the initial password, and enters a new password in the form provided. Once this process is complete, the new user can log in to the Webroot account.
Editing Account Settings

An account defines your user details such as login name, password, etc., and access permissions. You can add or change any of the account settings, except the email address specified for your login name.

This topic contains the following procedures:

- Editing Account Settings
- Adding Your Name, Number, or Time Zone
- Changing Your Password
- Changing Your Security Code
- Changing Your Security Question

To edit account settings:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16

2. Click the Down arrow at the right of your login ID, then select Account Settings.

SecureAnywhere displays the Account Settings page.
3. Click any of the **Change** links to edit information.

### Adding Your Name, Phone Number, or Time Zone

If needed, you can add your name, contact information, and the time zone where your PCs are located. You can also include a Display Name, which displays in the Manage Users panel. For more information, see *Adding Users on page 29.*
1. Access your account settings as described above.

2. Click the **Change** link to the right of a name, phone, or time zone field.

   The Account Settings window displays.

![Account Settings window](image)

**Note:** As needed, you can deselect the **Use Security Code during log in** checkbox so that you or other users do not have to enter a two-digit security code when you log in.

3. Enter or change the information, then click the **Save Details** button.

   To change the time zone, click the **Pencil** icon to the right of the field, then type the country, region, or city to open a drop-down menu of choices.

4. If you are the Admin for your account, you can also change access rights by clicking **Access & Permissions**. For a description of permissions, see *Adding Users on page 29*.
Changing Your Password

You entered a password when you created the account. If needed, you can change it in the account settings.

1. Access your account settings as described above.
2. Click the Change link to the right of the Password field.

The Change Password window displays.
3. In the Current Password field, enter your current password.

4. In the New Password field, enter your new password.

   Your password must be at least nine characters long and contain at least six alphabetic characters and three numeric characters. Your password can be longer than the required nine characters. It can include special characters, except for angle brackets: < and >. Your password is case sensitive.

   As you type, the Strength meter shows how secure your password is. For optimum security, you should make your password as strong as possible.

5. In the Repeat New Password field, enter the same characters as you did in the New Password field.

6. When you're done, click the Change Password button.

**Changing Your Security Code**

You defined a security code when you created the account. As an extra security step, the SecureAnywhere website prompts you for this code right after you log in. If needed, you can change the code.

1. Access your account settings as described above.
2. Click Change to the right of the Security Code field.

   The Change Security window displays.
3. In the New Personal Security Code field, enter a word or number.

   Use a code that is easy to remember, using a minimum of six characters. Every time you log in, you must also enter two random characters of this code. For example, if your code is 123456 and it prompts you for the fourth and sixth character, you would enter 4 and 6. Your Personal Security Code is case sensitive.

4. In the Enter Password field, enter your current password.

5. When you're done, click the Change Security Code button.

   **Note:** As needed, you can deselect the Use Security Code during log in checkbox so that you or other users do not have to enter a two-digit security code when you log in. For more information, see step 3 in *Adding Users on page 29*.

**Changing Your Security Question**

The security question allows Webroot to identify your account if you forget your user name, password, or security code. If you answer the question correctly, we can retrieve the login information for you.
1. Access your account settings as described above.

2. Click **Change** to the right of the Security Question field.

   ![Account Settings](image)
   
The Change Security Question window displays.

   ![Change Security Question](image)

3. From the New Security Question drop-down menu, select a security question.

4. In the New Security Answer field, type an answer.

5. In the last field, enter your current password.

6. When you're done, click the **Change Security Question** button.
Chapter 4: Using PC Security

To use PC security, see the following topics:

- Viewing PC Statuses ................................................................. 42
- Adding PCs ........................................................................... 45
- Editing PC Security Settings .................................................... 48
- Viewing PC Scan Information .................................................. 53
- Scanning PCs Remotely ............................................................ 59
- Running System Optimizer Remotely ....................................... 65
- Deactivating PCs ..................................................................... 71
- Locking, Shutting, Down, or Restarting PCs ............................... 78
Viewing PC Statuses

From the website, you can globally review status information for your PCs. Status information includes scan results and license information.

**Note:** To view PC status, you must first install SecureAnywhere on the PC, enter your Webroot account credentials when prompted, then allow SecureAnywhere to run a scan.

To view the PC status:

1. Open your browser and go to [my.webrootanywhere.com](http://my.webrootanywhere.com). For more information, see *Logging In to Your Account on page 16*.
2. Click the **PC Security** tab or click the **Go to PC Security** button.

The PC Security panel displays, listing all the devices associated with this account.
3. You can customize what devices are displayed by selecting an option from the View drop-down. You can also switch between a list view and an icon view by clicking the Icon/List button in the upper right:
4. You can view more details by clicking an individual PC.

![Screenshot of an individual PC's details]

5. In the About panel, you can view details about recent scans, the software version, keycode, and days remaining on your license.

You can also remotely change the security setting. For more information, see Editing PC Security Settings on page 48.
Adding PCs

If you purchased a multi-license edition, you can install SecureAnywhere on additional PCs using the same keycode. The SecureAnywhere website will display information about these PCs after a scan runs on each one, as described in this section. If you used a different keycode to install SecureAnywhere, follow the instructions in Adding Devices With Different Keycodes on page 20.

To view all PCs associated with your account:

1. Install SecureAnywhere on each PC, using your multi-seat license keycode.
2. When SecureAnywhere prompts for your account information, enter your user name, which is your email address, and password.
3. At the end of the installation routine, wait for SecureAnywhere to finish scanning the PC. Do not cancel the scan.

   Once the PC is scanned, SecureAnywhere reports into your account and adds the PC to the account website.

4. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.

   The new PC displays in the PC Security panel. By default, SecureAnywhere displays the machine name
5. Click the newly installed PC’s icon to open its information panel.

![PC Security Panel](image)

The Security panel for that computer displays.

![Security Panel](image)
6. To change the PC's displayed name, click the **Edit** link, enter a new name, and click the green checkmark to the right of the field.
Editing PC Security Settings

You can use the SecureAnywhere website to remotely change a PC's security setting to a higher or lower level of protection, as described in this section. These levels of protection are a combination of SecureAnywhere's heuristic settings, which include:

- **Advanced Heuristics** — Analyzes new programs for suspicious actions that are typical of malware.

- **Age Heuristics** — Analyzes new programs based on the amount of time the program has been in the community. Legitimate programs are generally used in a community for a long time, but malware often has a short life span.

- **Popularity Heuristics** — Analyzes new programs based on statistics for how often the program is used in the community and how often it changes. Legitimate programs do not change quickly, but malware often mutates at a rapid pace. Malware may install as a unique copy on every computer, making it statistically unpopular.

These heuristic settings are applied to separate areas of your computer, including the local drive, USB drives, the Internet, the network, CD/DVDs, and when your computer is offline. For more information, see [Adjusting Heuristics](#) in the Webroot SecureAnywhere PC User Guide.

By default, PC security is set to User Configuration, which means that you can control the settings from the SecureAnywhere main interface on the PC. If you use the SecureAnywhere website to switch the security from User Configuration to one of the other levels, it overrides SecureAnywhere's local settings on the PC.

To edit the PC security setting:

1. Open your browser and go to [my.webrootanywhere.com](http://my.webrootanywhere.com). For more information, see [Logging In to Your Account on page 16](#).
2. Click the **PC Security** tab or click the **Go to PC Security** button.

The PC Security panel displays.
3. Click the PC you want to modify.

The Security panel for that computer displays.
4. In the Security Setting line, click the **Edit** link.

![Security Settings](image)

5. Click the drop-down arrow to open protection options.

To learn about what the four levels of protection will provide such as low, medium, high, or maximum, click the blue question mark next to Security Setting to display an information panel.

![Protection Options](image)

6. Select from these options:
   - **User Configuration** — Security settings are controlled by the main interface on the computer.
   - **Low** — All heuristics are set to Low. This is limited protection, which might be convenient for software developers and highly technical users who run beta versions of software and don't want those applications being blocked.
- Medium — Heuristics are set to our recommended combination of Low, Medium, and High. This setting is for normal, daily use.

- High — All heuristics are set to High. Only use this setting if you suspect the PC is at risk. This setting results in a high number of alerts, which may block legitimate programs as well as malware.

- Maximum — Most heuristics are set to Maximum. Only use this setting if you suspect the PC is infected. This setting results in a high number of alerts, which may block legitimate programs as well as malware.

7. Click the Green checkmark to apply the new setting.

If you change a setting to Low, Medium, High, or Maximum, it overrides SecureAnywhere's local settings on the PC.
Viewing PC Scan Information

You can remotely view detailed scan results for each PC in your account. Details include whether your computers are secure or infected.

To view scan information for a PC:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.
2. Click the PC Security tab or click the Go to PC Security button.

The PC Security panel displays.
3. Click the PC you want to view.

The Security panel for that computer displays.
### WINDOWS8

<table>
<thead>
<tr>
<th>Last Scan</th>
<th>Mar 18, 2015 12:44</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Scan Duration</td>
<td>Approx. 34 secs</td>
</tr>
<tr>
<td>Last Infected</td>
<td>Never Infected</td>
</tr>
<tr>
<td>Software Version</td>
<td>8.0.7.33</td>
</tr>
<tr>
<td>Keycode</td>
<td>XXXX-XXXX-XXXX-XXXX</td>
</tr>
<tr>
<td>License Duration</td>
<td>190 Days Remaining</td>
</tr>
<tr>
<td>Security Setting</td>
<td>User Configuration</td>
</tr>
</tbody>
</table>

*Protected*
4. Click the **Scan Information** tab.

- The Scan Results panel displays the results of the last 10 scans on the PC, including the date and time, and the IP address the computer used.
- The Recent Malicious files detected panel displays information for the last 10 malicious files that were detected on the PC.
5. For more information about an infection, click the **View Bads** link on the main Scan Results tab.

Another panel opens with the file name and the threat category, for example, Trojan, Adware, etc..
Scanning PCs Remotely

You can remotely scan a PC, if you are away from your computer and you suspect it might be infected, for example, you are at work and a family member contacts you that the computer is acting strangely.

To scan a PC remotely:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.
2. Click the PC Security tab or click the Go to PC Security button.

The PC Security panel displays.
3. Click the **PC** you want to scan.

The Security panel for that computer displays.
### Chapter 4: Using PC Security

[Image of a security software interface showing details such as Last Scan, Last Scan Duration, Last Infected, Software Version, Keycode, License Duration, and Security Setting.]

**Windows 8**

<table>
<thead>
<tr>
<th>Last Scan</th>
<th>Mar 18, 2015 12:44</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Scan Duration</td>
<td>Approx. 34 secs</td>
</tr>
<tr>
<td>Last Infected</td>
<td>Never Infected</td>
</tr>
<tr>
<td>Software Version</td>
<td>8.0.7.33</td>
</tr>
<tr>
<td>Keycode</td>
<td>XXXX-XXXX-XXXX-XXXX</td>
</tr>
<tr>
<td>License Duration</td>
<td>190 Days Remaining</td>
</tr>
<tr>
<td>Security Setting</td>
<td>User Configuration</td>
</tr>
</tbody>
</table>

- 61 -
4. Click the **Commands** tab.

The Commands panel displays.
5. Click one of the following scan types:
   
   - **Scan** — Runs a scan on the PC and notifies you if it detected any threats, which allows you to decide whether to quarantine the files or not.
   
   - **Cleanup** — Runs a scan on the PC and automatically quarantines files without notifying you.
6. At the prompt, click the **Confirm** button.

   The scan will run on the computer as soon as it receives the command, which should only take a minute or two.
Running System Optimizer Remotely

You can remotely run the System Optimizer on a PC, if you are away from your computer and want to guard your privacy or hide your Internet traces, for example, you are at work and a family member wants to use your personal computer.

**Note:** For more information about the System Optimizer, see [Changing System Optimizer Settings](#) in the [WSA PC User Guide](#).

**To remotely run the System Optimizer on a PC:**

1. Open your browser and go to [my.webrootanywhere.com](http://my.webrootanywhere.com). For more information, see *Logging In to Your Account on page 16.*
2. Click the **PC Security** tab or click the **Go to PC Security** button.

The PC Security panel displays.
3. Click the **PC** you want to clean.

The Security panel for that computer displays.
4. Click the **Commands** tab.

The Commands panel displays.
Chapter 4: Using PC Security

![Diagram of PC security commands]

- **Scan**
  - Scan the PC

- **System Optimizer**
  - Run the System Optimizer

- **Restart PC**
  - Restart the PC

- **Deactivate**
  - Deactivate this computer

- **Cleanup**
  - Scan and quarantine malicious files

- **Lock PC**
  - Lock the PC

- **Shutdown PC**
  - Shutdown the PC
5. Click the **System Optimizer** button.

The cleanup will run on the computer as soon as it receives the command, which should only take a minute or two.

6. At the prompt, click **Confirm**.
Deactivating PCs

Deactivating a PC removes it from the PC Security panel and removes the SecureAnywhere application from that computer. You may want to deactivate a PC if you:

- No longer use a PC that had SecureAnywhere installed.
- Are replacing a PC with a new machine and you want to transfer the license.

**Note:** Deactivating a PC is not reversible; that is, you cannot reactivate a PC without reinstalling the software.

To deactivate SecureAnywhere on a PC:

1. Open a browser and go to my.webrootanywhere.com.
2. Enter your email address and password and click the Log in button.
3. Click the **PC Security** tab or the **Go to PC Security** button.

The PC Security panel displays.
4. Click the **PC** you want to deactivate.

![Computer Security Panel](image1)

The Security panel for that computer displays.

![Security Panel Details](image2)
5. Click the **Commands** tab.

The Commands panel displays.
6. Click the **Deactivate** button.

The Confirm window displays.

---

**Deactivate**

Are you sure you wish to deactivate this computer?

Deactivating a computer will stop it from being shown under the default PC list. This should be used to hide old machines which are no longer used, or where the Webroot software has since been uninstalled.

- **Confirm**
- **Cancel**
7. Click the **Confirm** button.

The system removes the computer from the PC Security list, and uninstalls Webroot SecureAnywhere application from the computer selected.
Locking, Shutting, Down, or Restarting PCs

You can remotely lock, shut down, or restart a remote PC from the website interface.

To issue one of these remote commands:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.
2. Click the PC Security tab or click the Go to PC Security button.

The PC Security panel displays.
3. Click the PC you want to lock, shut down, or restart.

The Security panel for that computer displays.
4. Click the **Commands** tab.

![Commands panel]

The Commands panel displays.
5. From here, you can issue one of the following commands:
   - **Lock** — Locks the PC by activating the Windows Login screen. A user name and password must be entered to log back in.
   - **Restart** — Restarts the PC.
   - **Shutdown** — Shuts down and turns off the PC.
6. At the prompt, select one of the following:
   - Lock
   - Restart
   - Shutdown

7. At the prompt, click **Confirm**.

   The computer should receive the command in a minute or two.
Chapter 5: Using Mobile Security

To use PC security, see the following topics:

- Adding Mobile Devices .............................................................. 85
- Viewing Mobile Account Information ......................................... 86
- Viewing Mobile Security Statuses and Alerts ............................... 88
- Viewing Mobile Histories ........................................................... 90
- Using Lost Device Protection Commands ................................. 92
- Changing Phone Numbers ........................................................ 96
- Removing Mobile Devices ......................................................... 98
Adding Mobile Devices

You can add Android smartphones, tablets, and other mobile devices to your Webroot account. You must first install one of the SecureAnywhere apps, which you can obtain by:

- Purchasing a SecureAnywhere edition that includes a license for mobile apps. These editions include Complete and Internet Security Plus.
- Purchasing the standalone Premier app for Android devices.
- Downloading the free app for Android devices.

To download and install Webroot apps, see the following knowledgebase article: http://www5.nohold.net/Webroot/Loginr.aspx?login=1&app=vw&solutionid=903.

Note: Website support for iOS devices is coming soon.

After you register the mobile device or create a Webroot account from the app, the device information will display in the SecureAnywhere website. For more information, see Viewing Mobile Account Information on page 86.
Viewing Mobile Account Information

From the website, you can view mobile account information, including the keycode and license status.

To view the mobile account information:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.
2. Click the Mobile Security tab or click the Go to Mobile Security button.

3. In the Mobile Security panel, you can view more details by clicking an individual device.

If needed, you can switch between a list view and an icon view by clicking the Icon/List button in the upper right:
When the About panel displays, you can view details about the device model, keycode, and days remaining on your license.

4. To change the displayed name for your device, click the **Edit** link. Enter a new name and click **Save**.
Viewing Mobile Security Statuses and Alerts

You can view detailed status and alerts for your mobile devices.

To view mobile security status:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.
2. Click the Mobile Security tab or click the Go to Mobile Security button.
3. Click on the mobile device.

   If needed, you can switch between a list view and an icon view by clicking the Icon/List button in the upper right:
4. Click the **Security Status** tab.

![Security Status Tab](image)

5. If your device is in a warning state, you can view more information by clicking the **X items need attention** link:

![Alerts and Fix Options](image)

You can only fix an issue from the SecureAnywhere app on your mobile device. The main panel will provide options for fixing the issue.
Viewing Mobile Histories

You can view a history of activity on the device, including information on the scan history and threat definition updates.

To view mobile history:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.

2. Do one of the following:
   - Click the Mobile Security tab
   - Click the Mobile Security button
3. Click on the mobile device for which you want to view the history.

   ![Image of a mobile device with options to click and an icon/list button](image)

   If needed, you can switch between a list view and an icon view by clicking the **Icon/List** button in the upper right:

4. Click the **History** tab.

   ![Image of a mobile security app's history tab](image)

   You can view a history for the past 7 Days, 30 Days, 60 Days, or 90 Days.
Using Lost Device Protection Commands

Delete this text and replace it with your own content. Lost Device Protection helps you lock and locate a missing mobile device. You can issue the commands from the SecureAnywhere website or from another smartphone.

Note: Lost Device Protection commands will lock down your phone. To unlock it, you must enter your Webroot password. Make sure you remember your password before issuing the command.

To issue a Lost Device Protection command:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.

2. Do one of the following:
   - Click the Mobile Security tab
   - Click the Go to Mobile Security button

3. In the Mobile Security panel, click an individual device to view additional details.

   To switch between a list view and an icon view, click the Icon/List button in the upper right:
4. At the top of the panel, click the **Lost Device Protection** tab.
5. In the Lost Device Protection panel, select from one of the following commands.

<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock</td>
<td>Remotely locks the device and prevents its unauthorized use. Once it's locked, you must use your account password to unlock it.</td>
</tr>
</tbody>
</table>
| Wipe (Premier/Complete version only) | Immediately locks the device, then performs a factory reset to remove everything on your device, including your personal data, your apps, and your account.  
Do not use this command unless you are absolutely sure that your device is permanently lost and you want to completely wipe it.  
Before wiping data, SecureAnywhere turns off the Auto-sync function so it won't delete anything you have previously uploaded to the Gmail servers, such as contacts or calendar entries. |
| Locate                 | Locks your device, which is the same as the Lock command, described above, then responds with a link to a Google Maps page that displays your device's current location.  
**Note:** For the Locate command to work, the device must have either a GPS, Wi-Fi, or a telephony connection. Also, if your device does not support SMS or if Webroot does not support your carrier, then you must have logged into the Android Marketplace. |
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scream</td>
<td>Locks your phone, which is the same as the Lock command, described above, and then blasts a loud screaming noise from your phone to help you locate the device or scare a thief. The noise will continue for up to two minutes or until you unlock the device with your password.</td>
</tr>
<tr>
<td>Customize Lock Screen</td>
<td>Locks your phone, which is the same as the Lock command, described above, and displays a text message on its panel. When you use this command, you can enter instructions for returning the phone, such as If found, call 555-5555.</td>
</tr>
</tbody>
</table>
Changing Phone Numbers

If you change your phone number, you can enter the new number in the SecureAnywhere website.

To change a phone number:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.

2. Do one of the following:
   - Click the Mobile Security tab
   - Click the Go to Mobile Security button

3. Click on the mobile device.
To switch between a list view and an icon view, click the **Icon/List** button in the upper right:

![Icon/List button](image)

4. Next to the displayed phone number, click the **Edit** link.

![Edit link](image)

5. Enter the new number and click **Save**.
Removing Mobile Devices

If you no longer use a mobile device displayed in the SecureAnywhere website, you can remove it from the list.

To remove a mobile device:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.

2. Do one of the following:
   - Click the Mobile Security tab.
   - Click the Go to Mobile Security button.

3. In the Mobile Security panel, click on the mobile device you want to remove.
To switch between a list view and an icon view, click the **Icon/List** button in the upper right:

4. Below the device image, click the **Remove This Device** button.

Note: Be aware that removing a device from the website does not uninstall the app from your phone or tablet. If you power on the device again later and it checks back in with the SecureAnywhere app, the device displays in this website.
Chapter 6: Using Backup And Sync

To use Backup & Sync, see the following topics:

Backup & Sync Overview ...................................................... 101
Storing Files in the Anywhere Folder or in Your Own Sync Folders ...................................................... 101
Backing Up Files ................................................................. 102
Getting Started With Backup & Sync ........................................ 103
Managing Files and Folders ...................................................... 105
  Renaming Files ................................................................. 105
  Moving Files ................................................................. 106
  Deleting Files or Folders ...................................................... 107
  Creating Folders ............................................................ 108
Customizing Displays ............................................................ 110
  Switching Views ............................................................ 110
  Customizing Folder Displays .............................................. 111
  Refreshing Data ............................................................. 111
Restoring Files From the Recycle Bin ........................................ 113
Downloading Files From Your Account ...................................... 115
Uploading Files and Folders ..................................................... 117
Viewing Version Histories ..................................................... 119
Viewing Device Details .......................................................... 121
Viewing Activity Logs .......................................................... 124
Using the Windows Store App for Backup & Sync ......................... 126
Viewing Account Details ........................................................ 129
Backup & Sync Overview

If your SecureAnywhere edition includes Backup & Sync, you can protect your important files and photos as described in this topic.

Storing Files in the Anywhere Folder or in Your Own Sync Folders

You can use Webroot's preconfigured folder called the Anywhere folder or you can create your own sync folders. Any files you place in these folders are automatically synchronized in your account, to any other computers with shared folders, and to mobile devices with the Backup & Sync app installed.

SecureAnywhere constantly monitors the Anywhere folder and other sync folders. If it detects a change such as an edited file, a new file, or a deleted file, it immediately makes the same change to your online account, to shared folders on other computers, and to mobile devices with the Backup & Sync app installed. If you are working offline, SecureAnywhere automatically picks up changes the next time you connect to the Internet.
If SecureAnywhere detects an edited file, it does not overwrite the original version stored in your account. Instead, it uploads the latest version and makes a copy of the original file. If necessary, you can revert back to previous versions, up to five. If you save changes a sixth time, your most recent version is saved and the oldest version is removed.

For more information about the preconfigured Anywhere folder, see Adding Sync Folders in the WSA PC User Guide, or Adding Sync Folders in the WSA Mac User Guide.

**Backing Up Files**

Instead of synchronizing files with multiple devices, you can simply back them up. For example, you may want to back up tax returns, old photos, and a scanned copy of your passport. These types of documents won’t change and don’t need to be kept in synchronization with other computers.

To learn more about backups, see Managing Backup & Sync in the WSA PC User Guide, or Managing Backup & Sync in the WSA Mac User Guide.
Getting Started With Backup & Sync

With the Backup & Sync app installed, and from the SecureAnywhere website. These instructions provide procedures for using Backup & Sync features available from the website. For detailed information about using Backup and Sync features from the main interface or your mobile device, see Webroot SecureAnywhere Help and Product Guides.

To get started with Backup & Sync:

1. If you have not yet created an account in the SecureAnywhere website, click the Sign up now button in the Create an Account panel.
   For more information, see Creating Accounts on page 8.

2. Open SecureAnywhere on your computer and make sure the Backup & Sync component is configured. Repeat this process for all computers associated with your account.
   For more information, see the WSA PC User Guide or the WSA Mac User Guide.

3. You can install the Backup & Sync app on your mobile devices.
   For more information and instructions on installing the apps on your mobile devices, see Download Instructions.

4. Once Backup & Sync is configured on your computers and mobile devices, access your online account by logging in to my.webrootanywhere.com.

5. From the Home panel of the website, click the Go to Backup & Sync button

The Backup & Sync web page displays.
The Backup & Sync page includes three tabs across the top:

- **Files and Folders** — Displays synchronized and backed up files. From this tab, you can upload and download files; view, move, delete, and rename files; and perform other tasks. For more information, see *Managing Files and Folders on page 105* and *Customizing Displays on page 110*.

  **Note:** Any changes, deletions, or additions you make in the synchronized folders are also propagated to your online SecureAnywhere account and to other synchronized folders on other computers.

- **Activity log** — Keeps track of all Backup & Sync activity for this account. For more information, see *Viewing Activity Logs on page 124*.

- **Devices** — Displays details about your backed up and synchronized devices. For more information, see *Viewing Device Details on page 121*. 
Managing Files and Folders

From the SecureAnywhere website, you can manage files or folders by renaming, moving, deleting, and adding them. Be aware that if you make these changes to the Anywhere folder or another sync folder, all changes are propagated to your computers and mobile devices with SecureAnywhere installed.

This topic contains the following procedures:

- Renaming Files
- Moving Files
- Deleting Files or Folders
- Creating Folders

Renaming Files

You can rename a file from the website. Be aware that if you are renaming a synchronized file or folder, the change will be propagated across all synchronized devices.

To rename a file:

1. Select the file you want to rename.
2. Do either of the following:
   - Right-click the file name, and then select Rename.
   - Click the Rename icon.
3. When SecureAnywhere prompts for the new name, enter the new name and click **Apply**.

![File Management Table]

**Moving Files**

You can move a file to a different folder from the website. Be aware that if you are moving a synchronized file or folder, the change will be propagated across all synchronized devices.

**To move a file:**

1. Do either of the following to select files you want to move:
   - Click on the file you want to move.
   - Press **Ctrl-Click** to highlight multiple files.

2. Do either of the following to move the files:
   - Right-click on the filename, and then select **Move**.
   - Click the **Move** icon.

![File Manager Interface]

SecureAnywhere displays the Move To window, showing the destination options for the move.
3. Select the new destination folder and click Select.

SecureAnywhere displays a progress bar while performing the move.

Deleting Files or Folders

You can delete a file or folder from the website. Be aware that if you are deleting a synchronized file or folder, the change will be propagated across all synchronized devices. Deleted files are moved to the Recycle Bin where you can recover them later, if necessary. If you empty the Recycle Bin to permanently delete the files or folders, the files are also removed from the computer and you cannot recover them.

To delete a file or folder:

1. Click on the file you want to delete, or press **Ctrl-Click** to highlight multiple files.
2. Do either of the following:
   - Right-click and select Delete.
   - Click the Delete icon.
3. When SecureAnywhere prompts for a confirmation, click **OK**.

**Creating Folders**

You can create a new folder from the website. Be aware that if you are adding a subfolder to a synchronized folder, the change will be propagated across all synchronized devices.

**To create a folder:**

1. Highlight the storage folder where you want to create a new folder.
2. Click the **Create New Folder** icon.
3. When SecureAnywhere prompts for a name, enter a name and click **Apply**.

![Image of SecureAnywhere interface](image)

The new folder is added to the storage folder.
Customizing Displays

Within the Files and Folders page, you can switch from a details to images view, sort data, and refresh data.

This topic contains the following procedures:

- Switching Views
- Customizing Folder Displays
- Refreshing Data

Switching Views

For folders that contain images, you can switch between detail view and image view. To display a detailed view, click the Detail icon.

To display an image view, click the Image icon.
Customizing Folder Displays

While you are in detail view, you can move columns and change the sorting order.

To move a column:
1. Grab the column header by left-clicking on it.
2. Drag the column to its new location.

To change the sorting:
1. To select a column as the sort by column, click the column heading.
2. Optionally, run the pointer over the column heading.
   A Down arrow displays.
3. Click the Down arrow to display the menu and select either Sort Ascending or Sort Descending.

Refreshing Data

You may want to refresh data to make sure you have the latest version of files from all devices synchronized with this account.

To refresh data:
1. Click the **Refresh** icon.
Restoring Files From the Recycle Bin

When you delete a file from a storage container, the system moves it to a SecureAnywhere Recycle Bin for that specific storage container. If you accidentally deleted files or folders, you can retrieve them from the Recycle Bin.

To restore a file or folder from the Recycle Bin:

1. Open a browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.
2. Click the Go to Backup & Sync button.
3. From the left panel, select the folder where you previously deleted the file.
4. Select Actions > View Recycle Bin.
5. When the file and folders in the Recycle Bin display, right-click the file or folder you want to restore, then click Restore.
Note: To permanently delete files from the Recycle Bin, you can select **Actions > Empty Recycle Bin**. Be aware that if you empty the Recycle Bin, you can never recover the files. Also, if you delete a synchronized file or folder, it is removed from the computer and you cannot recover it.
Downloading Files From Your Account

Using any device with an Internet connection, you can download files residing in your Anywhere folder, a sync folder, or the Backup folder. For example, if you are traveling and need access to a file, simply log in to your SecureAnywhere account and download the file. You can download a single file or a group of files as a Zip archive, as described below.

This topic contains the following procedures:

- **Downloading Single Files**
- **Downloading Large or Multiple Files or Folders**

To download a single file:

1. From the left panel, select the folder that contains the file you want to download.
2. In the center panel, right-click the file you want to download.
   
   SecureAnywhere displays a menu of actions.
3. Click **Download**.

   ![Download Icon]

   SecureAnywhere asks if you want to Open, Save or Cancel the download.

4. Do one of the following:
   - To save the file, click **Save** and browse to the folder on your local device where you want to save the file.
   - To open the file, click **Open**.
SecureAnywhere searches for the file's associated program and opens it.

To download large or multiple files and/or folders:

1. Press **Ctrl-click** to highlight the files or folders you want to download.
2. Right-click the files to open the menu and select **Download as Zip Archive**. Or click the **Download as Zip** button.

   ![File List](image)

   SecureAnywhere asks if you want to open or save the group of files and folders.

3. Click **Save**.
Uploading Files and Folders

From any browser, you can manually upload files and folders to your online account in the SecureAnywhere website. The Upload feature is convenient if you are traveling and are away from your main computer. You can place files in the Anywhere folder or another sync folder to immediately synchronize files to your computer and mobile devices. You can also place files in the Backup folder for archival.

To upload a file or a folder:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.

2. Click the Go to Backup & Sync button.

3. From the left panel, select the destination folder.

4. Click the Upload icon.

SecureAnywhere displays the Upload Files window.
5. Click **Select Files** and browse to the file you want to upload.

6. Browse to and select the file or folder.

   The Upload progress displays in the window.

7. Do either of the following:
   - Repeat the above steps to upload additional files or folders,
   - Click **Close** to exit the window. When you click Close, the uploaded files are added to the folder.
Viewing Version Histories

You can save up to five previous versions of a file. If you save changes a sixth time, your most recent versions are saved and the oldest version is removed. You can download any of those saved versions.

To view the version history:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.

2. Click the Go to Backup & Sync button.

3. Right-click on the file whose version history you want to view, and select Show Versions.

The Version History panel displays. The first file, Index 0, is the most current version.
4. If needed, you can do either of the following:
   - Download a previous version by right-clicking on its row and clicking **Download**.
   - Reset a file to the current version by selecting **Set Current** or remove an old version by clicking **Delete**.
Viewing Device Details

The Devices tab displays information about each device with Backup & Sync configured. It also displays the storage folders associated with each device.

To display details about a device:

1. Open a browser and enter the following URL:
   
   my.webrootanywhere.com

   For more information, see *Logging In to Your Account on page 16*.

2. Click the **Go to Backup & Sync** button.

3. At the top of the page, click the **Devices** tab.
4. Click on an individual device. The device's details window displays.

![Device Details Window]

The table below provides descriptions for the device details.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>About Tab</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Title</strong></td>
<td>By default, SecureAnywhere displays the host name. Click the <strong>Edit</strong> link to change the name, then click the <strong>Green</strong> checkmark to save the new name.</td>
</tr>
<tr>
<td><strong>Host Name</strong></td>
<td>The host name of the device.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Last Connected</td>
<td>The date and time this device was last synchronized.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of device, such as Desktop Computer.</td>
</tr>
<tr>
<td>Deauthorize</td>
<td>Click the X to disconnect this device from the account.</td>
</tr>
<tr>
<td>Storage Folders Tab</td>
<td></td>
</tr>
<tr>
<td>Folders</td>
<td>Displays a list of synchronized folders associated with this device.</td>
</tr>
</tbody>
</table>
Viewing Activity Logs

The Activity Log keeps track of all user activity for all folders and devices associated with your account.

To view the Activity Log:

1. Open your browser and go to my.webrootanywhere.com. For more information, see Logging In to Your Account on page 16.
2. Click the Go to Backup & Sync button.
3. Click the Activity Log tab at the top of the screen.

An activity log displays.

The following table provides descriptions for each column.
<table>
<thead>
<tr>
<th>COLUMN</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>The date and time the activity was performed.</td>
</tr>
<tr>
<td>Activity</td>
<td>The type of activity performed.</td>
</tr>
<tr>
<td>Item</td>
<td>The file or folder name associated with the activity.</td>
</tr>
<tr>
<td>Storage Folder</td>
<td>The name of the Storage Folder where the activity took place.</td>
</tr>
<tr>
<td>By User</td>
<td>The SecureAnywhere account ID of the user.</td>
</tr>
<tr>
<td>Via Device</td>
<td>The name of the device where the activity took place. This will either</td>
</tr>
<tr>
<td></td>
<td>indicate a device name or display WebPortal for activity that took place</td>
</tr>
<tr>
<td></td>
<td>from the website.</td>
</tr>
</tbody>
</table>
Using the Windows Store App for Backup & Sync

If you purchased a multi-license edition, you can download the Backup & Sync Windows Store app to a Windows 8 or RT device.

**Note:** For more information and instructions, see the Backup & Sync Windows Store App User Guide.

To download and install the Windows Store app:

1. From the Windows Start screen, select the Store tile.
2. From the Store, go to the Productivity category.
3. Locate the Webroot Backup & Sync app and select Install.
4. When you see the Webroot tile on your desktop, select the tile to open Backup & Sync.

5. At the first screen, enter your Webroot account login credentials and your keycode.

   The Backup & Sync app synchronizes with your Webroot account in the cloud. If you have folders in your account, you will see those folders display, similar to the following example:
The Backup & Sync app provides options for managing your files and folders, as described below:

A taskbar provides options for adding files, refreshing the display, selecting all files, viewing details, and creating a new folder. This taskbar is available at the bottom of the panel. When a folder view is displayed, the following options display.

If a file is selected, additional options display that allow you to delete files, clear selections, and save files:

The Charms bar provides access to Backup & Sync settings. Move your mouse to the bottom, right corner to display these options. Click Settings to access the Backup & Sync settings, which allows you to view app information, access Help, view account settings, and change permissions.
The following Backup & Sync Settings display.
Viewing Account Details

To view information about your Backup & Sync account, follow this procedure.

To view account details:

1. In the upper right corner of the window, click the Information icon.

The system displays the Account Details panel that shows your account details, storage space, and user details.
Account Details

- Account ID: XXXX-XXXX-XXXX-XXXX
- Account Name: Standard123456
- Storage Region: 200
- Account Storage Space: 25 GB
- Total Space Used: Less than 1 MB used
- User ID: XXXX-XXXX-XXXX-XXXX
- User Name: JohnDoe@gmail.com
- User Display Name: JohnDoe@gmail.com
- Space Used by User: Less than 1 MB used
# Chapter 7: Working With Passwords

To work with passwords, see the following topics:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Getting Started With Passwords</td>
<td>132</td>
</tr>
<tr>
<td>Using the Password Manager Toolbar</td>
<td>135</td>
</tr>
<tr>
<td>Accessing Passwords From Your Account</td>
<td>142</td>
</tr>
<tr>
<td>Capturing Login Credentials</td>
<td>146</td>
</tr>
<tr>
<td>Capturing Login Credentials While in a Website</td>
<td>146</td>
</tr>
<tr>
<td>Defining Login Credentials From the SecureAnywhere Website</td>
<td>152</td>
</tr>
<tr>
<td>Capturing Additional Login Credentials</td>
<td>155</td>
</tr>
<tr>
<td>Logging in to Password-Managed Sites</td>
<td>160</td>
</tr>
<tr>
<td>Generating Secure Passwords</td>
<td>165</td>
</tr>
<tr>
<td>Editing Password-Managed Sites</td>
<td>168</td>
</tr>
<tr>
<td>Importing and Exporting Data</td>
<td>174</td>
</tr>
<tr>
<td>Importing Passwords From Other Applications</td>
<td>174</td>
</tr>
<tr>
<td>Exporting User Names And Passwords</td>
<td>177</td>
</tr>
<tr>
<td>Using Form Fill Profiles</td>
<td>180</td>
</tr>
<tr>
<td>Creating Form Fill Profiles</td>
<td>180</td>
</tr>
<tr>
<td>Populating Fields With Form Fill Profiles</td>
<td>184</td>
</tr>
<tr>
<td>Editing Form Fill Profiles</td>
<td>185</td>
</tr>
<tr>
<td>Setting Preferences</td>
<td>189</td>
</tr>
<tr>
<td>Using Other Browsers</td>
<td>195</td>
</tr>
</tbody>
</table>
Getting Started With Passwords

If your SecureAnywhere edition includes Passwords, you can use the following features:

- Capture user names and passwords and populate them automatically when you access a website.
- Set up a profile you can use to populate more extensive web forms automatically, such as credit card payment forms.
- Generate secure passwords for all your commonly-used websites.

With the Password Manager, you will never need to remember multiple login names and passwords, write them down on paper, or store them in an unencrypted file on your device. Plus, the Password Manager works across all your devices, including laptops, mobile phones, and tablets.

Note: To keep your data safe from hackers, the Password Manager encrypts all your personal data on your local computer. SecureAnywhere uses the same encryption method employed by the US Government for Top Secret data. The encrypted data is meaningless to Webroot and to anyone else.
without the decryption key. This key is stored on your own computer and is created using your email address and master password. This personal data is never sent over the Internet.

To get started with Passwords:

1. If you have not yet created an account in the SecureAnywhere website, click the **Sign up now** in the Create an Account panel.
   
   For more information and instructions, see *Creating Accounts on page 8*.

2. Make sure the Passwords component is configured. If not, the button on the Home panel of the website says **Set Up Account Now**.

   Click the **Set Up Account Now** button and follow the prompts to complete the process. When the Passwords component is configured, the Set Up Account Now button changes to Go to Passwords. This may take about 15 minutes.

3. Click the **Go to Passwords** button.

   The Password Management page displays.
4. If you have a multi-user license, you can install the SecureWeb app on additional computers and mobile devices for password management. For instructions on installing the apps on your mobile devices, see Download Instructions.

   Once the Passwords component is configured on your computers and mobile devices, those users can access the online account by logging in to my.webrootanywhere.com.

5. Make sure all appropriate user accounts have Passwords enabled Access. For more information, see Adding Users on page 29.
Using the Password Manager Toolbar

To enable Webroot Password functions while you work on the Internet, you log in from the Webroot Password drop-down menu in your browser's toolbar. When you are signed in from the drop-down menu, SecureAnywhere can automatically populate your login credentials for sites that require a user name and password. The menu also allows you to access favorite sites, auto-populate data into web forms, and perform other tasks.

The Webroot icon for the Passwords menu displays differently, depending on your browser. The following is an example of the Firefox icon and menu.

![Webroot Password Manager Toolbar](image)

**Note:** If the Webroot Passwords icon and associated drop-down menu do not display in your browser, make sure it is enabled in the browser's Add-Ons /Extensions list.

To use the Password Manager toolbar:

1. Open your Internet browser.
2. After you have Password Management set up, a Webroot SecureAnywhere icon displays in the toolbar of your browser, which provides a drop-down menu of Password Management features. Initially, the icon is grayed-out.
Webroot Icon in Chrome

Webroot Icon in Firefox

Webroot Icon in Internet Explorer

**Note:** If you do not see the icon in your browser, reboot your machine. If you still don't see the icon, check your browser's Add-On or Extensions settings and make sure the Webroot apps are enabled. If you are using a browser other than Firefox, Internet Explorer, or Chrome, see *Using Other Browsers on page 195.*

3. To activate the Password Management functions for use as you browse the Internet, click the icon and log in using your SecureAnywhere account login credentials.

4. Once you have logged in, the Webroot icon turns green. Click the icon or the arrow next to it to display the menu of features.
Webroot Icon in Chrome

Webroot Icon in Firefox

Webroot Icon in Internet Explorer

5. These features are now available as you browse and shop and conduct other business on the Internet:

Chrome Main Menu
Firefox Main Menu
Internet Explorer Main Menu

<table>
<thead>
<tr>
<th>File</th>
<th>Edit</th>
<th>View</th>
<th>Favorites</th>
<th>Tools</th>
<th>Help</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Search Webroot Vault
- Sites
- Form Fills
- Generate Secure Password
- Recently Used
- Tools
- Preferences
- Help...

Logoff: JohnDoe@gmail.com

6. From this menu, you can log in to your sites, populate forms with personal data, save data entered into forms, and set preferences for the Password Manager.

See the following table for more information.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logoff</td>
<td>Logs out of your Webroot SecureAnywhere account.</td>
</tr>
<tr>
<td>Recently Used</td>
<td>Click the arrow to access a list of password-managed sites that you recently visited.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sites</td>
<td>Click the arrow to access a list of all password-managed sites that you</td>
</tr>
<tr>
<td></td>
<td>defined, organized by group. If you did not specify a group for a site,</td>
</tr>
<tr>
<td></td>
<td>that group is listed under (none).</td>
</tr>
<tr>
<td></td>
<td>Sites allows you to save credentials while the website is loaded; the</td>
</tr>
<tr>
<td></td>
<td>Password Manager will save as much data as it can from the website fields</td>
</tr>
<tr>
<td></td>
<td>currently displayed.</td>
</tr>
<tr>
<td>Fill Forms</td>
<td>Click the arrow to access fill form commands.</td>
</tr>
<tr>
<td></td>
<td>You can use a fill form profile to populate fields in the currently</td>
</tr>
<tr>
<td></td>
<td>displayed website, edit or delete a fill form profile, add a fill form</td>
</tr>
<tr>
<td></td>
<td>profile, and clear fields in a form.</td>
</tr>
<tr>
<td>Preferences</td>
<td>Displays the Preferences window where you can modify the behavior of the</td>
</tr>
<tr>
<td></td>
<td>Password Manager.</td>
</tr>
<tr>
<td></td>
<td>For more information, see Setting Preferences on page 189.</td>
</tr>
<tr>
<td>Help</td>
<td>Opens the Webroot SecureAnywhere Help website.</td>
</tr>
</tbody>
</table>
**FIELD** | **DESCRIPTION**
--- | ---
**Tools** | Click on Tools to access the following:
- **Generate Secure Password** — For information, see *Generating Secure Passwords on page 165.*
- **Refresh Sites** — If you edited site information and the changes don't display immediately, click **Refresh Sites** to force the changes.
- **Import From** — For information, see *Importing and Exporting Data on page 174.*
- **Export To** — For information, see *Importing and Exporting Data on page 174.*
- **Print** — Allows you to print your password-managed site information.
- **Clear Local Cache** — If you use the Password Manager from a public computer, the encrypted data is stored on that computer. Select **Clear Local Cache** to remove any files stored during your session.
- **Add Site** — For information, see *Capturing Login Credentials on page 146.*

**Save All Entered Data** | Allows you to capture and save additional login data, such as account number.

For more information, see *Capturing Login Credentials on page 146.*
Accessing Passwords From Your Account

You can access all your saved credentials and other personal information from your account in the SecureAnywhere website. In the Passwords page, you can also edit information you saved for logins, form-fills, and favorite sites.

To access a password from your account:

1. Log in to my.webrootanywhere.com.
2. Click the Go to Passwords button.

The Passwords page displays. When you begin saving login credentials and organizing them in groups, the definitions are listed in the Sites tab.

3. Populate the fields using the information in the following table.
<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites</td>
<td>Provides a list of password-managed sites. You can edit, open, or delete previously defined sites and the groups you created for them. For more information, see Capturing Login Credentials on page 146.</td>
</tr>
<tr>
<td>Favorites</td>
<td>Provides a list of sites you have designated as a favorite when you captured login credentials for the site. You can view, edit, and delete sites in your Favorites list.</td>
</tr>
<tr>
<td>Form Fill profiles</td>
<td>Provides a list of profiles you have defined to fill in forms. You can view, edit, and delete Form Fill profiles. For more information, see Using Form Fill Profiles on page 180.</td>
</tr>
<tr>
<td>Passwords</td>
<td>Provides a list of generated passwords. You can view, edit, and delete generated passwords. For more information, see Generating Secure Passwords on page 165.</td>
</tr>
<tr>
<td>MyIdentity actions &gt; Add site</td>
<td>Allows you to manually define login credentials for a password-managed site. For more information, see Capturing Login Credentials on page 146.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>MyIdentity actions &gt; Add group</strong></td>
<td>Allows you to define a group for password-managed sites. Groups help you organize sites into categories for easier viewing. When you add a group, it is added to the group drop-down list available for selection when you define credentials on a website.</td>
</tr>
<tr>
<td><strong>MyIdentity actions &gt; Add a Form Fill profile</strong></td>
<td>Allows you to define a profile that will be used to populate forms automatically. A profile includes such personal information as your name, address, and credit card numbers. This feature saves you from manually typing your personal data into web forms every time you make an online purchase, complete a survey, and so on. For more information and instructions, see <em>Using Form Fill Profiles on page 180</em>.</td>
</tr>
<tr>
<td><strong>MyIdentity actions &gt; Open all Favorites</strong></td>
<td>Allows you to open sites that you specified as Favorites. All the sites open at once in separate tabs of your web browser, which can be convenient if you use the Passwords page as your browser’s home page.</td>
</tr>
<tr>
<td><strong>MyIdentity actions &gt; View deleted items</strong></td>
<td>Allows you to view and recover any groups or sites you previously deleted.</td>
</tr>
<tr>
<td><strong>MyIdentity actions &gt; View history</strong></td>
<td>View a list of tasks you performed with the Password Manager.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **MyIdentity actions > View Never list** | Allows you to suppress the toolbar prompts for specific websites.  
In the dialog, select the type of prompts to suppress and enter the websites where you do not want to see those prompts. |
| **MyIdentity actions > Install Bookmarklets** | Allows you to create Bookmarklets, which help you access data if you are traveling, have a mobile browser, or are using an unsupported browser.  
For more information, see *Using Other Browsers on page 195*. |
| **MyIdentity actions > Import data** | Allows you to import data from another password-management application.  
For more information and instructions, see *Importing and Exporting Data on page 174*. |
| **MyIdentity actions > Export data** | Copies your user names and passwords into an Excel spreadsheet.  
For more information and instructions, see *Importing and Exporting Data on page 174*. |
| **Recently visited sites** | Displays a list of recently visited sites. |
| **Open all recently visited sites** | Opens all sites listed in your Recently visited sites list. |
Capturing Login Credentials

When you are logged in to your SecureAnywhere account and access a website that requires a username and password, the Password Manager automatically detects any information you enter into login fields and prompts you to capture the credentials. Later, when you open that website again, the Password Manager can populate the fields or log you in automatically.

This topic contains the following procedures:

- Capturing Login Credentials While in a Website
- Defining Login Credentials From the SecureAnywhere Website
- Capturing Additional Login Credentials

Capturing Login Credentials While in a Website

To capture login credentials:

1. Make sure you are logged in to your SecureAnywhere account. Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password. If you are not logged in, you will be prompted to do so.

   Webroot Icon in Chrome

   ![Webroot Icon in Chrome](image)

   Webroot Icon in Firefox

   ![Webroot Icon in Firefox](image)
Webroot Icon in Internet Explorer

2. Open a website that requires login credentials, such as a banking site, an account with an Internet vendor, or a social media site.

3. Log in to the site with your user name and password.
   As the site logs you in, the Password Manager detects the user name, password, and URL. It then prompts you to save the login information from a green toolbar near the top of your browser.

4. From the prompt, click Save Site.

The Add Webroot Site window displays with the web address already displayed in the Name field. The user name, password, and URL have been saved automatically and do not display in this window.

Add Webroot Site - Chrome
Add Webroot Site - Firefox
Add Webroot Site - Internet Explorer
5. Optionally, you can specify more information about the site and how you want to access it in the future, as described in the following table:
### FIELD | DESCRIPTION
---|---
Name | The web address is used for the site name, unless you want to change it to something simple, such as My Credit Union.
Group | You can define a name for a group or select one from the list, if you already defined groups.
  
  By defining a group, you can organize sites by categories, such as Banking and Shopping.
  
  If you do not enter a group, the site is categorized in a default group.
Make This a Favorite | If you access this site frequently and are storing login credentials for numerous sites, select this checkbox to save this site to your Favorites list.
  
  You can quickly access your Favorites using the Open all Favorites option from the Passwords page.
Require Password Reprompt | Select this checkbox if you don't want your password automatically populated, but want to manually enter the password yourself. This setting also requires you to enter your SecureAnywhere master password before editing the site information.
AutoLogin | To bypass the password prompt and log in automatically, select this checkbox.

6. Click the **Save Site** button.

The system saves the information, which you can then view in your online SecureAnywhere account.
The next time you access this website, make sure you are signed in to your SecureAnywhere account so the Password Manager can automatically populate in your login credentials. For more information, see Logging in to Password-Managed Sites on page 160.

Defining Login Credentials From the SecureAnywhere Website

To define login credentials:

1. Log in to my.webrootanywhere.com and click the Go to Passwords button.

2. On the far right of the panel, under MyIdentity actions, select Add site.
3. At the prompt, click **Yes, let me manually add a site**.

The Add site window displays.
4. Populate the fields using the information in the following table.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name for the website, for example, enter My Bank. This name is displayed in SecureAnywhere prompts.</td>
</tr>
<tr>
<td>Group</td>
<td>Define a name for a group or select one from the list, if you already defined groups. By defining a group, you can organize sites by categories in the Passwords page and in the SecureWeb apps, such as Banking and Shopping. If you do not enter a group, the site is categorized in a default group.</td>
</tr>
<tr>
<td>URL</td>
<td>Enter the URL of the website’s login page, for example, enter the following: <a href="http://www.website.com/login">http://www.website.com/login</a></td>
</tr>
<tr>
<td>User name</td>
<td>Enter your login name for the site.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter your password for the site.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Notes</td>
<td>Enter any extra information that might be helpful, such as your PIN number for a bank account. This is an optional step.</td>
</tr>
<tr>
<td>Options</td>
<td>If needed, select any of the following checkboxes:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Show in Favorites</strong> — If you access this site frequently, select this checkbox to create a Favorites list. You can then use the Open all Favorites option from the Passwords page.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Reprompt for password</strong> — Select this checkbox if you don't want your password automatically populated, but want to manually enter the password yourself. This setting also requires that you enter your SecureAnywhere master password before editing the site information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Automatically fill</strong> — Select this checkbox if you want your user name and password automatically populated when you access the site. Otherwise, deselect this checkbox.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Automatically log in</strong> — To bypass the password prompt and log in automatically, select this checkbox.</td>
</tr>
</tbody>
</table>

5. Click the **Add site** button.

The next time you access this website, make sure you are signed in to your SecureAnywhere account so the Password Manager can automatically populate in your login credentials. For more information, see [Logging in to Password-Managed Sites on page 160](#).

**Capturing Additional Login Credentials**

Some websites require more than a user name and password for a login, such as the last four digits of your social security number or medical plan number. If you frequently access a site with additional login credentials, you can use Save All Entered Data to capture those extra fields.
To capture additional login credentials:

1. Make sure you are logged in to your SecureAnywhere account. Click the **Webroot** icon in your browser's toolbar, then enter your SecureAnywhere user name and password.

   **Webroot Icon in Chrome**

   ![Webroot Icon in Chrome](image)

   **Webroot Icon in Firefox**

   ![Webroot Icon in Firefox](image)

   **Webroot Icon in Internet Explorer**

   ![Webroot Icon in Internet Explorer](image)

2. Open the website and populate the required fields.

3. From the SecureAnywhere drop-down menu in the browser, select **Save All Entered Data**.

   **Save All Entered Data - Firefox**
Chapter 7: Working With Passwords

Save All Entered Data - Internet Explorer
The Edit Site Information window displays. This window contains information that it captured from the site. It captures all the fields it can, even if you did not enter information in those fields.
4. When you're done making changes, click the **OK** button.

The next time you access this website, make sure you are signed in to your SecureAnywhere account. The Webroot SecureAnywhere icon displays at the end of the fields to indicate that the login credentials are stored in the Password Manager. For drop-down fields, the icon is not shown.
Logging in to Password-Managed Sites

After you define login credentials for a site, the Password Manager can automatically log in to the site from a web browser on a computer or from the SecureWeb app on a mobile device.

This topic contains the following procedures:

- Logging In to a Site From Browsers
- Logging In to a Site From Website

To log in to a site from a browser:

1. Log in to your SecureAnywhere account. Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.

   **Chrome**

   ![Chrome](image)

   **Firefox**

   ![Firefox](image)

   **Internet Explorer**
2. You can log in to a site from the browser toolbar or by opening the website.

**Note:** If you defined more than one login for a single website, each login displays separately in the list of sites.

- **Toolbar** — From the Webroot SecureAnywhere toolbar, open the drop-down menu, click **Sites**, and select a password-managed site from the list.

**Chrome**

![Chrome screenshot]

**Firefox**

![Firefox screenshot]
Internet Explorer
- Website — In your browser, open the website and click the Login button. The Password Manager remembers how you defined the site. For example, if you specified auto-fill, it automatically enters the login credentials for you. The Webroot SecureAnywhere icon displays at the end of the fields to indicate that the login information is stored in the Password Manager. The user name and password fields are automatically populated, unless you selected the Require Password Reprompt checkbox in the Add Webroot Site window.

To log in to a site from the SecureAnywhere website:

1. Log in to my.webrootanywhere.com and click the Go to Passwords button.
The Passwords page displays, with your password-managed sites listed in the Sites tab.

2. To open a site, from the Sites tab, click on the site name.

   If you specified a site as a favorite, you can access it from the Favorites tab. You can also select **Open all Favorites** from MyIdentity actions.
Generating Secure Passwords

You can use the Password Manager to generate a strong, hack-resistant password for any website. A strong password is difficult to guess and helps protect you from identity theft. You don't need to remember these automatically generated passwords. When you access this web page again, the Password Manager automatically populates the password field for you.

To generate a secure password:

1. Log in to your SecureAnywhere account. Click the Webroot icon in your browser's toolbar, then enter your SecureAnywhere user name and password.

   **Chrome**

   ![Chrome screenshot](image)

   **Firefox**

   ![Firefox screenshot](image)

   **Internet Explorer**

   ![Internet Explorer screenshot](image)
2. Access a password-protected web page and click inside the password field. The Password Manager toolbar displays.

3. From the toolbar, click Generate.

If this toolbar doesn’t display, click the drop-down arrow next to the icon, then select Tools > Generate Secure Password.

The Generate Secure Password window displays with a generated password.

4. If you want a different password than the one shown, you have several options:
   - To create another password, click the Generate button, then click the Accept button. You can keep clicking Generate until you are satisfied with the password displayed in the field.
To display more options for password generation, select the **Show Advanced Options** checkbox. Select the items you want, then click the **Generate** button. You can keep clicking **Generate** until you are satisfied with the password displayed in the field, then click the **Accept** button.

5. Click the **Accept** button to use the randomly generated password currently shown in the field.

If you are not logged in or you are not accessing a web page with a password field, a Copy button displays instead of the Accept button. Click **Copy** to copy the password to your clipboard. You can then paste the password into a password field.

Once you click the **Accept** button, the new password is populated into the Password and Confirm Password fields in your web page.

For more information about viewing or changing passwords, see *Editing Password-Managed Sites on page 168.*
Editing Password-Managed Sites

You can modify captured site information from a web browser on a PC or Mac, or from the Passwords page of your SecureAnywhere account.

To edit password-managed sites:

1. Open a web browser.
2. Use one of the following methods to edit a password-managed site:
   - **Toolbar** — Sign in to your SecureAnywhere account. Access the site you want to edit. From the drop-down menu, select the site name at the bottom, then click **Edit**.

   **Chrome**
Firefox
Internet Explorer

- 170 -
Passwords page in your SecureAnywhere account — Log in to my.webrootanywhere.com and click Go to Passwords. Locate the row for the site you want to change, then click Edit.

The Edit Site Information window displays. This window looks slightly different if you loaded it from the Passwords page. Depending on what information you originally defined for the site, this window may display different fields.
3. Use the information in the following table to populate the fields.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>URL</td>
<td>The URL of the website's login page, which should not be modified unless the URL has changed.</td>
</tr>
<tr>
<td>Name</td>
<td>The site name.</td>
</tr>
<tr>
<td>Group</td>
<td>A group you defined and assigned to this site, if any.</td>
</tr>
<tr>
<td>User name</td>
<td>Your login name for the site.</td>
</tr>
<tr>
<td>FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>Your password for the site. To see the actual password characters, click <strong>Show</strong>.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>Any extra information about this site, such as a PIN number.</td>
</tr>
<tr>
<td><strong>Options</strong></td>
<td>Do any of the following, as needed:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Favorite</strong> — Select this checkbox if you access this site frequently and want to add it to your favorites list. You can then use the Open All Favorites feature from the Passwords page.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Require Password Reprompt</strong> — Select this checkbox if you don't want your password automatically in the field, and instead, want to manually enter the password yourself. This setting also requires that you enter your SecureAnywhere master password before editing the site information.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Never AutoFill</strong> — Select this checkbox if you do not want the fields in the website automatically populated when you access the site.</td>
</tr>
<tr>
<td></td>
<td>- <strong>AutoLogin</strong> — Select this checkbox if you want to bypass a password prompt and go directly to the web page.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Fields/Edit Form Fields</strong> — If this site includes fields that were captured with Save All Entered Data, the fields display in this form. There may also be a link to Edit Form Fields.</td>
</tr>
</tbody>
</table>
Importing and Exporting Data

You can import passwords into SecureAnywhere from another password-management application or export data from SecureAnywhere to an Excel file.

This topic contains the following procedures:

- Importing Passwords From Other Applications
- Exporting User Names And Passwords

Importing Passwords From Other Applications

If you are currently using another password-management application, you can import data from that application into SecureAnywhere’s Password Manager.

To import passwords from another application:

1. Open a web browser.
2. You can either use the toolbar or the Passwords page, as follows:
   - **Toolbar** — Sign in to your SecureAnywhere account. From the Webroot SecureAnywhere drop-down menu, select Tools, then Import From. A list of applications displays in a submenu. In the submenu, select from the list of password-management applications.

Firefox Path
Internet Explorer Path
Passwords page in your SecureAnywhere account — Log in to my.webrootanywhere.com and click Go to Passwords. Under MyIdentity actions, select Import data.
3. From the dialog, click the arrow next to the **Import data from** field and select the appropriate password-management application.

4. Click **Continue**.

5. Follow the on-screen instructions for importing passwords from that application.

   Since every password application is unique, the instructions for importing data from each one is also unique.

**Exporting User Names And Passwords**

You can use the Export feature to transfer all your Password Manager data into an HTML file, XML file, or a CSV file that can be opened using Microsoft Excel. The Export function is available from the Passwords page or from the drop-down menu in a browser.

**To export data from a browser:**

1. Log in to your SecureAnywhere account. Click the **Webroot** icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.

2. From the drop-down menu, select **Tools > Export To**.

**Firefox Path**

![Firefox Path Image](image-url)
3. Select one of the export options.

   A window displays asking for your SecureAnywhere master password.

4. Enter your SecureAnywhere account password and click **Sign In**.

5. Do one of the following:
   - If you selected Webroot CSV File or Webroot Encrypted File, the system prompts you for a file name and a directory to store that file.
   - If you selected a browser, your password data will be exported into the browser’s built-in password manager.

**To export data from the Passwords page:**

1. Log in to [my.webrootanywhere.com](http://my.webrootanywhere.com) and click **Go to Passwords**.
2. Under MyIdentity actions, click **Export data**.
3. From the dialog, enter your SecureAnywhere master password and click **OK**.
4. The Export Data window displays with all the information for your sites, passwords, and form-fill profiles. When you export data, data from all three tabs is exported to the output file.

5. Do one of the following:
   - Click **Save to File**.
   - Click **Send to Printer**.

   If you are saving a file, another window displays that allows you to select a file format.

6. Click **Export Data**.

7. If you are printing the data, your data is saved to an HTML page and another window displays where you can select a printer and click **OK**.
Using Form Fill Profiles

You can use SecureAnywhere’s Password Manager to automatically populate web forms with personal information that you commonly enter in fields, including your name, address, and credit card information. For example, you may want to create a personal profile with all your contact information, and several profiles for each credit card you use for Internet shopping. Then you can use a personal profile to automatically populate your name and address in the fields, and another profile to automatically populate your credit card information.

This topic contains the following procedures:

- Creating Form Fill Profiles
- Populating Fields With Form Fill Profiles
- Editing Form Fill Profiles

Creating Form Fill Profiles

Before you can populate web fields with personal information, you must first create a Form Fill profile. You can create a profile from the website browser or from the Passwords page of your SecureAnywhere account.

To create a Form Fill profile:

1. Open a web browser.
2. Use one of the following methods to create a Form Fill profile;
   - **Toolbar** — Sign in to your SecureAnywhere account. Access the site you want to edit. From the drop-down menu, select Fill Forms > Add Profile or select Fill Forms > Add Credit Card.

Chrome
Firefox
Internet Explorer
- Passwords page in your SecureAnywhere account — Log in to my.webrootanywhere.com and click Go to Passwords. Click the Form Fill profiles tab. Under MyIdentity actions, select Add Form Fill profile. Then select either Add Full profile or Add Credit Card profile.
The Form Fill profile window displays. The window looks slightly different if you selected it from the Passwords page. If you selected Add Credit Card, only the Credit Card Information and Notes tabs display in this window.

![Add Form Fill profile window](image)

3. In the Profile Name field, enter a name that defines this profile, such as *Personal Info* or *My Visa*.
4. Enter as much information as you want in each field. Click the tabs to move between panels.
   - The Custom Fields tab can be used to create fields that aren’t listed in this Form Fill dialog.
   - In Text to find, enter a field label from the website.
   - In Value to fill, enter the information you want automatically filled into that field.
   - Multiple lines are allowed, but keep in mind that multiple lines can only be filled into a multi-line field, not a single-line field.
5. To require a SecureAnywhere master password before editing the Form Fill information, select the **Require Password Reprompt** checkbox.
6. When you’re done, click the **OK** button.

**Populating Fields With Form Fill Profiles**

Once you define Form Fill profiles, you can use them to populate your personal information into web fields from a browser or from the SecureWeb app on a mobile device.
To populate a field with a form fill profile:

1. Access a website that requires you to enter personal information into fields, such as your name, address, credit card, etc.
2. Click in the first field.

   The yellow Password Manager toolbar displays. If this toolbar does not display, click the drop-down arrow next to the Webroot SecureAnywhere icon in your browser’s toolbar, then select **Fill Form > profile name > Fill Form**.

3. Click **Fill Form** and select the profile from the pop-up menu.

   To populate only specific fields, use your mouse to highlight the fields before you select the profile.

   ![Password Manager toolbar](image)

   The Password Manager transfers any information that applies to the fields.

**Editing Form Fill Profiles**

You can manage and access all your Form Fill profiles from a browser or from the Passwords page of your online SecureAnywhere account.

To edit Form Fill profiles:

1. Open a web browser.
2. You can either use the toolbar or the Passwords page in your SecureAnywhere account:
   - **Toolbar** — Sign in to your SecureAnywhere account. Access the site you want to edit. From the drop-down menu, select **Fill Forms**, the name of the profile you want to edit, then **Edit**.
   - **Chrome**
Firefox

Internet Explorer
- Passwords page — Log in to my.webrootanywhere.com and click Go to Passwords. Click the Form Fill profiles tab, then click Edit next to the profile you want to edit.
3. Edit the necessary information, then save your changes.
Setting Preferences

You can set several preferences for the Password Manager, such as how notifications display and what hotkeys you can use for shortcuts.

To set preferences:

1. Log in to your SecureAnywhere account. Click the Webroot icon in your browser’s toolbar, then enter your SecureAnywhere user name and password.

Webroot Icon in Chrome

![Webroot Icon in Chrome](image)

Webroot Icon in Firefox

![Webroot Icon in Firefox](image)

Webroot Icon in Internet Explorer

![Webroot Icon in Internet Explorer](image)
2. From the SecureAnywhere drop-down menu, select **Preferences**.

**Firefox Preferences**

![Firefox Preferences](image1)

**Internet Explorer Preferences**

![Internet Explorer Preferences](image2)
The Webroot Control Panel window displays.

Chrome

Firefox
3. Change the preferences as described in the following table.

When you’re done, click **OK**.
<table>
<thead>
<tr>
<th>SETTING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>Select whether you want to:</td>
</tr>
<tr>
<td></td>
<td>• Disable Insecure Firefox Password Manager. When selected, the Password Manager does not prompt you to save passwords.</td>
</tr>
<tr>
<td></td>
<td>• Open New Pages in... Select the current tab, Tabs, or Windows.</td>
</tr>
<tr>
<td></td>
<td>• Highlight Input boxes. When selected, the Password Manager displays fields in a different color.</td>
</tr>
<tr>
<td></td>
<td>• Automatically Fill Login Information. When selected, the Password Manager populates login fields with your user name and password.</td>
</tr>
<tr>
<td></td>
<td>• Default Form Fill Profile. Select the form-fill profile you want to use automatically and select the checkbox, if you do not want to overwrite fields that are already filled.</td>
</tr>
<tr>
<td></td>
<td>• Do not overwrite fields that are already populate. If this is enabled, fields containing data will not be filled in.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Select <strong>Notifications</strong> in the left panel. A descriptive list of notification options displays.</td>
</tr>
<tr>
<td></td>
<td>Select the checkboxes for each type of notification you want the Password Manager to display.</td>
</tr>
<tr>
<td>SETTING</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Hotkeys</strong></td>
<td>Select <strong>Hotkeys</strong> in the left panel, then enter key combinations you want to use for common Password Manager tasks.</td>
</tr>
</tbody>
</table>
| **Advanced** | Select **Advanced** in the left panel. A descriptive list of options displays. Select the checkboxes for the option you want to enable:  
  - If you frequently jump around from site to site, you might want to enable an auto-login. If you return to a site within the specified number of seconds, you will not have to log in again.  
  - Display a warning before filling insecure forms.  
  - Allow websites to disable AutoFill; keep the rule for AutoComplete=off.  
  - If you want the clipboard cleared automatically, select the number of seconds you want to elapse before it is cleared.  
  - Open a Webroot login dialog when you start the browser.  
  - Display an option to create new form-fill profiles automatically.  
  - Change the language displayed in dialog boxes, menus, and prompts. You must restart the browser. |
Using Other Browsers

To use a browser other than Internet Explorer, Firefox, or Chrome, you can create Bookmarklets to enable password functions. For example, to use Bookmarklets with Opera, you would drag Bookmarklet links to Opera’s Bookmarks Bar, then click on the bookmark to use automatic login. Bookmarklets can be used with Safari, Opera, Konqueror, and other browsers.

To use another browser:

1. Log in to my.wbrootanywhere.com and click the Go to Passwords button.
2. From the MyIdentity actions panel, select Install Bookmarklets.

The Bookmarklets window displays.
3. Click on a tab for the browser you want to use.

   Instructions for that browser display in the lower panel.

4. Follow the instructions to create the Bookmarklets, then click the OK button.

5. To use the Bookmarklet, go to your browser and click on the bookmark.

   The Password Manager either performs the function immediately or displays a window with more information.
Chapter 8: WSA Management Website Support

To access support, see the following topic:

Accessing Technical Support ................................................................. 198
Accessing Technical Support

Webroot offers a variety of support options. You can do any of the following:

- Is your Webroot subscription through Best Buy? Click here for additional support options.
- Look for the answer in our knowledgebase and FAQs.
- Look for the answer in our online documentation.
- Enter a help ticket.
- Connect to the Webroot Security for Android forum.
Index

A
accessing
  passwords 142
  technical support 198
account details, viewing 129
accounts, creating 8
activity logs, viewing 124
adding consoles 24
admin, default 8
answer, security 12, 26

B
Backup & Sync Windows store app, using 126
browsers 8

C
capturing login credentials 146
changing default console names 23
confirmation email 12
consoles
  adding 24
  managing 23
  switching between 27
creating
  accounts 8
  form fill profiles 180

D
data
  exporting 174
  importing 174
default admin 8
default console names, changing 23
device details, viewing 121
downloading files 115
E

editing
  form fill profiles 185
  password-managed sites 168
email, confirmation 12
exporting
  data 174
  passwords 177

F

files
  downloading 115
  uploading 117
folders, uploading 117
form fill profiles
  creating 180
  editing 185
  populating fields with 184
  using 180

G

generating secure passwords 165
getting started, passwords 132

I

importing
  data 174
  passwords 174

K

keycode, entering on registration 10, 25

L

logging in 16
  to password-managed sites 160
login credentials, capturing 146

M

managing consoles 23
O
other browsers, using 195

P

password-managed sites
  editing 168
  logging in to 160
password guidelines 11, 25
password manager toolbar, using 135

passwords
  accessing 142
  exporting 177
  getting started 132
  importing 174

personal security code 11, 26

populating fields with form fill profiles 184

preferences, setting 189

Q

question, security 11, 26

S
secure passwords, generating 165

security
  answer 12, 26
  code, personal 11, 26
  question 11, 26

setting preferences 189

switching between consoles 27

T

technical support, accessing 198

U

uploading
  files 117
  folders 117

using
  Backup & Sync Windows store app 126
  form fill profiles 180
other browsers 195
password manager toolbar 135

V

version histories, viewing 119
viewing
  account details 129
  activity logs 124
  device details 121
  version histories 119