WEBROOT SecureAnywhere BUSINESS SOLUTIONS

Getting Started with the Web Security Service

Webroot, Inc.
385 Interlocken Crescent, Suite 800
Broomfield CO 80021 USA
www.webroot.com

Contents

Overview

This document describes how administrators can get started with the Web Security Service. This service routes HTTP and HTTPs traffic through a web proxy located in Tier1 data centers. The web proxy will filter traffic based on configured policies, which block categories of websites that may infect corporate devices. Policies can also block other types of websites that employees should not access during working hours.

To begin configuration, follow the steps in this guide:

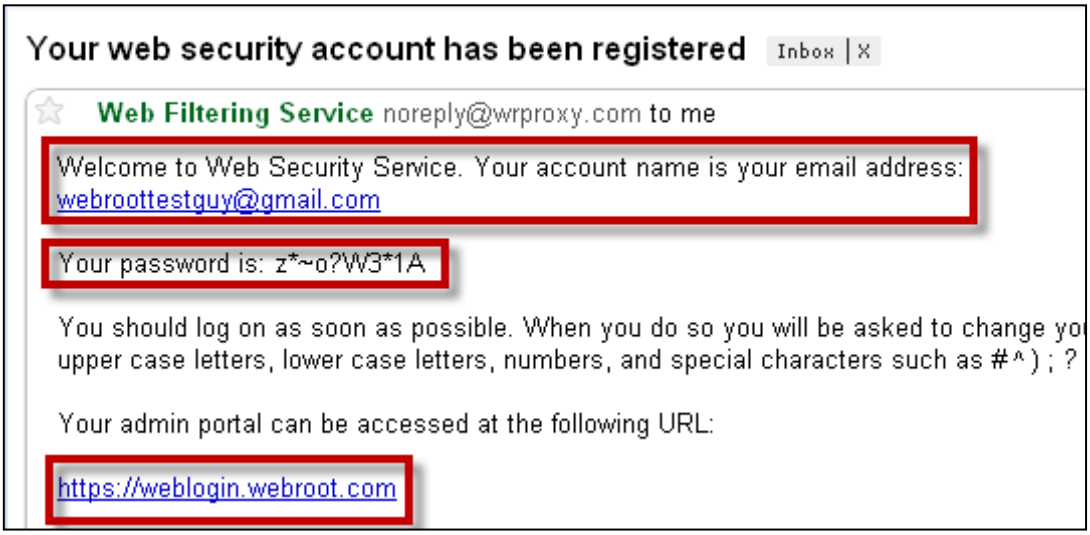
1. Log in to the Management Portal (Admin Console) and change your password.
2. Verify the IP address range of your account.
3. Configure web traffic filtering.
4. Modify policy settings and adjust filtering categories (optional).
5. Bypass web filtering for certain websites (if necessary).

Log in to the Management Portal

To manage the Web Security Service, you will use a web-based Management Portal (also called an "Admin Console"). The Management Portal is certified to work with the following browsers:

- Internet Explorer: versions 8, 9, and 10
- Firefox: the latest 5 versions
- Chrome: the latest 5 versions
- Safari: versions 5.0 and above
- Opera: the latest 5 versions

Your login credentials for the Portal are listed in a Welcome email that you received, similar to the example below. As a first step, you need to log in to the Portal and change your password.



To log in and change your password:

1. Log in to https://weblogin.webroot.com, using the credentials you received (your email address and the password generated for you).
   The Web Security Service prompts you to change the password.

2. Enter a new password that meets the following requirements: a minimum of 8 characters, with a mixture of 3 different types of characters (lower case, upper case, numbers, or special characters).
   The first time you log in, the Management Portal opens at the Profile tab's **General Information** subtab.

3. Check that your information is correct.
   (Optionally, you can also enter contact information.)

4. Click on the **Dashboard** tab.

From now on, you will see this dashboard every time you log in (see the following example). Once you configure web filtering, this dashboard will display traffic data in six different charts. The charts reflect data up to the current time, with a latency of approximately 15 minutes (depending on the service load).

You can control which charts appear in the dashboard. For more information, see the *Web Security Service Administrator Guide* or the *Management Portal Online Help*, which are available from the **Resources** tab at the top right of the dashboard. Click the **Documents** subtab to see the available user guides.

Verify the IP address range

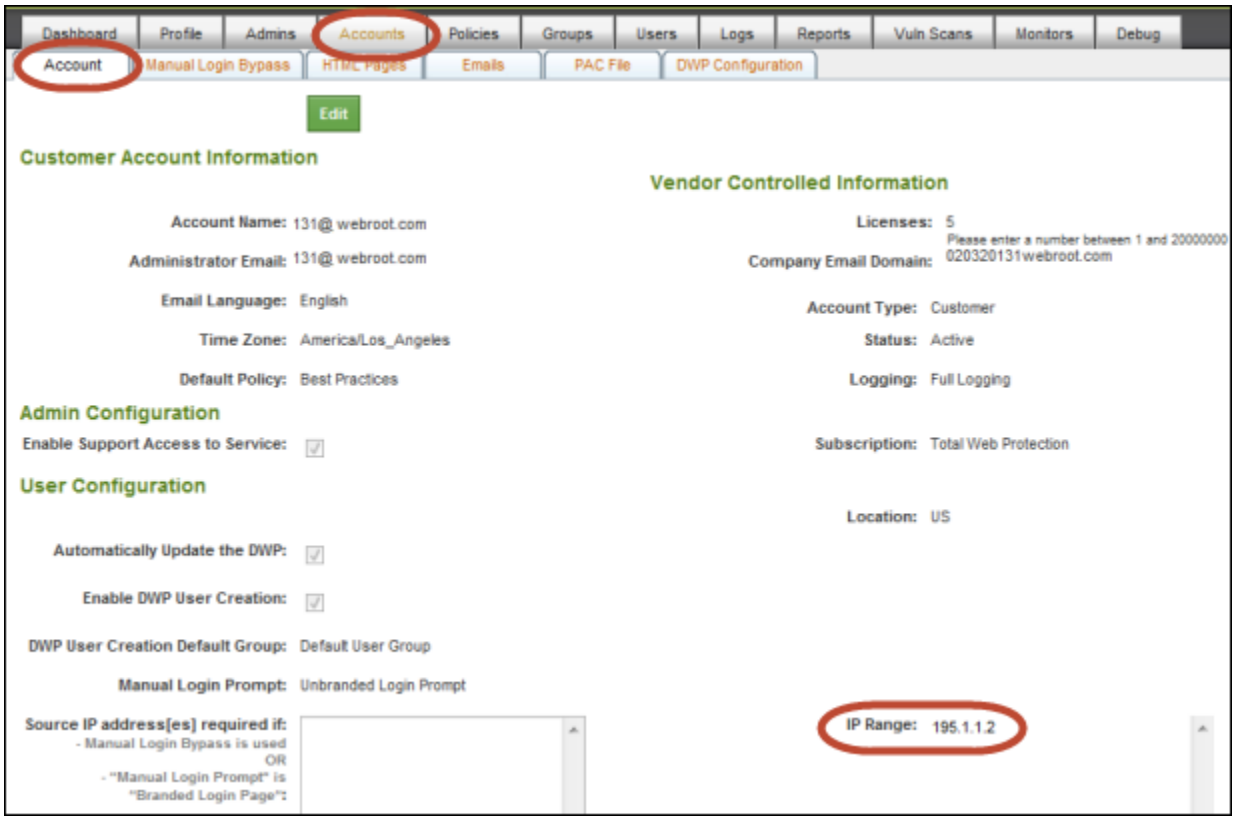
Next, verify that the corporate IP addresses are correct for your account.

> **Note:** Only your vendor can enter and modify the IP addresses. You cannot change them yourself.

To verify the IP address range:

1. Click on the **Accounts** tab, then make sure the **Account** subtab is selected.
2. In the lower right corner, locate the **IP Range** field, as shown in the following example. The service will use these IP addresses to intercept and filter traffic, so you must make sure the numbers are correct.

   > **Note:** You can check your computer's IP by opening a browser and connecting to www.whatismyip.com.



3. If the IP addresses listed on the account panel are **not** correct, contact your vendor. Only your vendor can modify this information.

Configure web traffic filtering

You can configure web filtering by using several methods:

- **Deploying the Desktop Web Proxy (DWP) to Windows computers**. If your network is comprised mostly of Windows-based systems, DWP offers the best method for quickly authenticating both on-site and remote systems. However, DWP *cannot* be installed on Macs, mobile phones, tablets, or Windows 8 devices.

- **Modifying LAN settings in users' browsers**. This is an ideal method for networks that include a mixture of Windows-based systems and other types of operating systems and devices. It's also ideal if you do not use your own gateway caching proxy or do any firewall redirections.

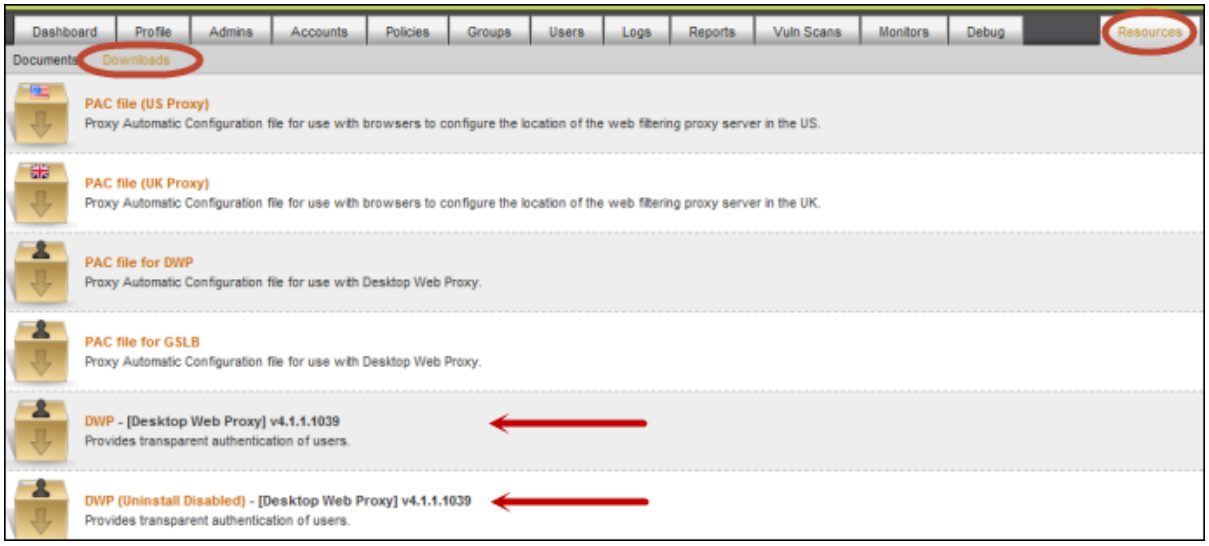
  Note: For some types of network setups, you can use the Management Portal to configure network-level filtering. With this method, you can enter the range of IP addresses in your network or upload the email addresses of all users. For more information, contact Technical Support or see the *Web Security Service Administrator Guide*.

Deploying DWP to Windows computers

You can install the Desktop Web Proxy (DWP) individually on each Windows workstation by using the **msi** installation package, a Group Policy Object editor, or another type of batch installation process. The .**msi** installation package for DWP is available from the Management Portal, on the **Resources>Downloads** tab.

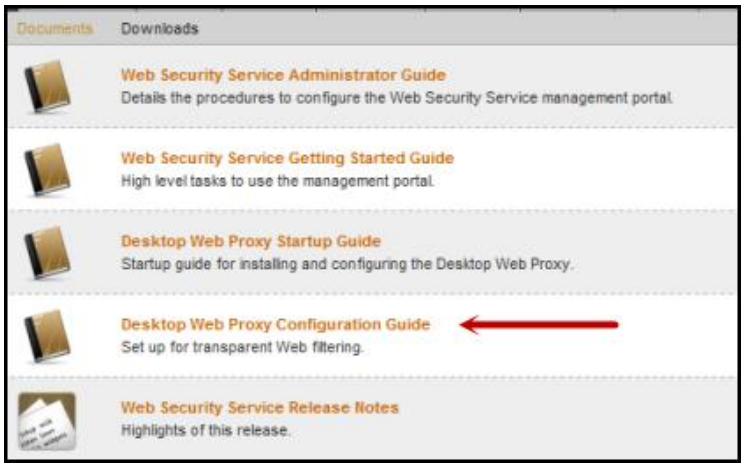
To download and install DWP:

1. In the Management Portal, click the **Resources** tab, then the **Downloads** subtab.



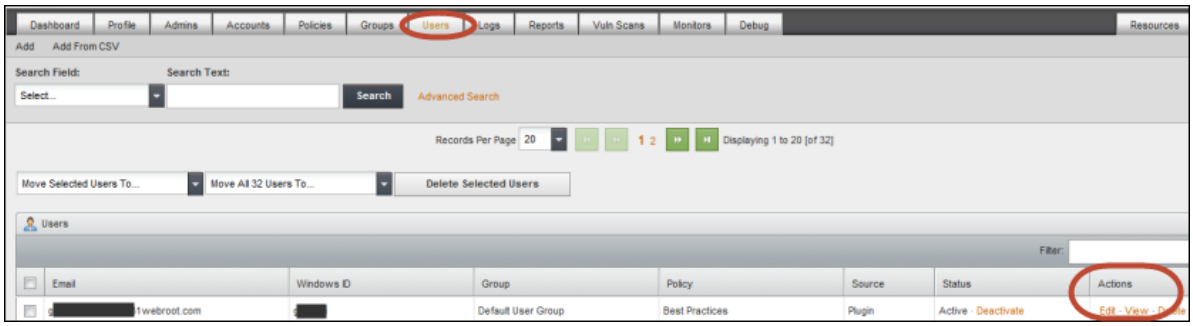
2. Click on one of the DWP files to save it.

3. Install and extract the DWP file on an individual Windows workstation or use a silent install to deploy DWP to multiple workstations.
   Deployment instructions are available in the *Desktop Web Proxy Configuration Guide*, available from the **Documents** subtab.



   After you deploy DWP, the DWP icon appears in the system tray of each computer:

4. From the Management Portal, click the **Users** tab and make sure all the users appear in the table. You can change information for a user by clicking the Edit link under the **Actions** column.



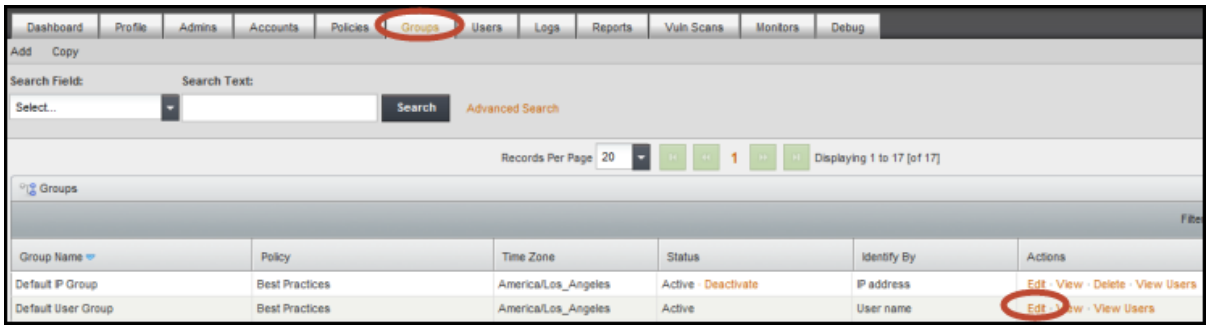
   All users are assigned to the Default User Group and Best Practices policy. If you want to change the policy settings and assignments, see “Modify policies and adjust filtering” on page 10.

Modifying LAN settings in users' browsers

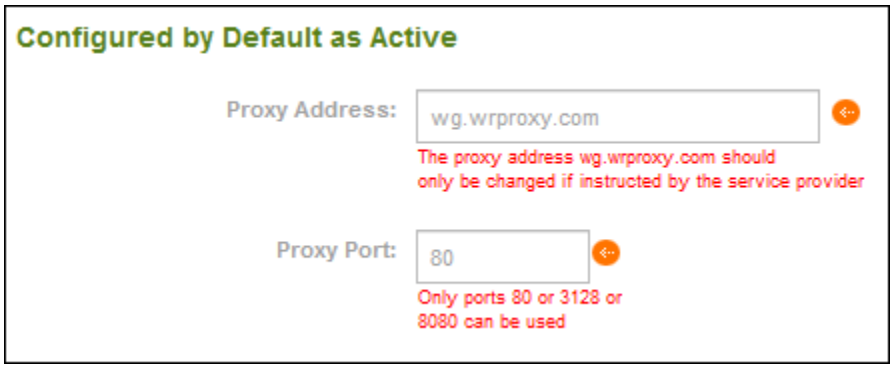
You can configure web filtering by entering a proxy URL and port in the browser for each workstation or other network device. The port number you enter depends on your configuration.

To check which port number to enter:

1. In the Management Portal, select the **Groups** tab.
2. Under **Actions**, locate the row for the **Default User Group**. On the far right, click the Edit link.



3. Click the **DWP Configuration** subtab.
4. Scroll down to "Configured by Default as Active."
   The number shown in the **Proxy Port** field is the number you must enter in LAN settings.



To configure browser-level web filtering:

1. From each workstation or other network device, open the browser and locate the LAN settings.
2. For the URL, enter: **wg.wrproxy.com**.
3. For the port number, enter **3128** or **80** or **8080**.
   It must match the number shown in the **Proxy Port** field of the **Groups>DWP Configuration** subtab.

4. For more detailed logs in the Management Portal, you can identify users by entering their email addresses. Use one of the following methods:

   - Synchronize with the LDAP directory.
   - Import users from a remote file.
   - Enter user information manually in the **Users** tab.
     For more information about entering user information, see the *Web Security Service Administrator Guide* or the *Management Portal Online Help*, which are available from the **Resources**>**Documents** tab.

   All users are assigned to the Default User Group and Best Practices policy. You can add more user-based groups and policies, if desired. If you want to change the policy settings and assignments, see the next section.

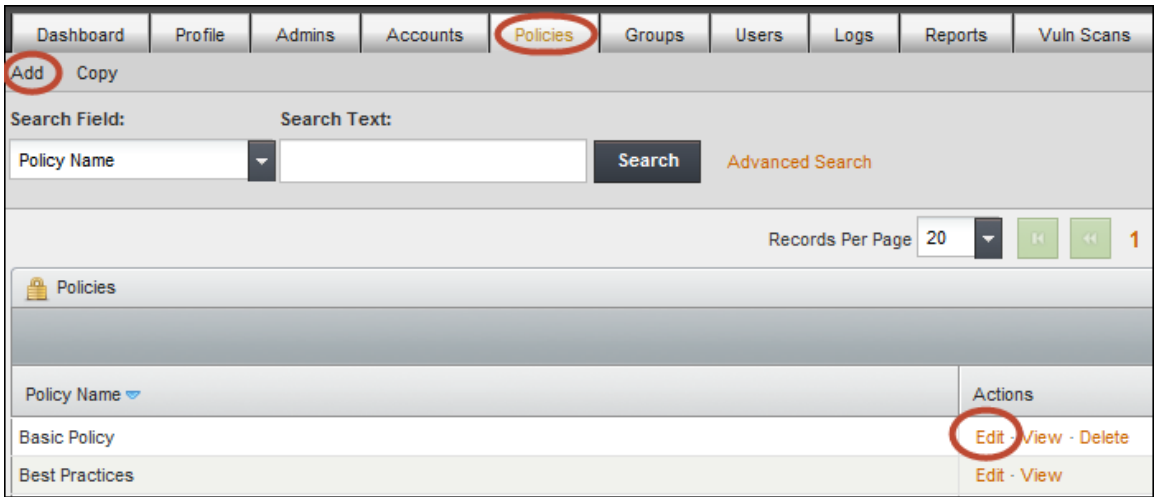
Modify policies and adjust filtering

Policies can control access to certain categories of websites or specific URLs. The Web Security Service includes several default policies for immediate use. If you want to customize these policies for your own requirements, follow the instructions in this section. Otherwise, you can skip this section.

> **Note:** Policies are assigned to default groups, which in most cases, are adequate to get started with the Web Security Service. For more information about modifying or adding groups, see the *Web Security Service Administrator Guide* or the *Management Portal Online Help*.

To add or modify policies:

1. Select the **Policies** tab.
   Each of the default policies appears in the lower panel.
2. You can click **Add** to create a new policy or click the Edit link in the Actions column to modify an existing policy.



3. From the Policy subtabs, you can block websites by category, block or allow specific sites, and block certain file types.
   For detailed instructions, see the *Web Security Service Administrator Guide* or the *Management Portal Online Help*.

4. Click **Save** when you're done.

   Note: If you added a new policy, you must assign it to a group. Go to the **Groups** tab, select the Edit link, and select the new policy.

Bypass web filtering for specific websites

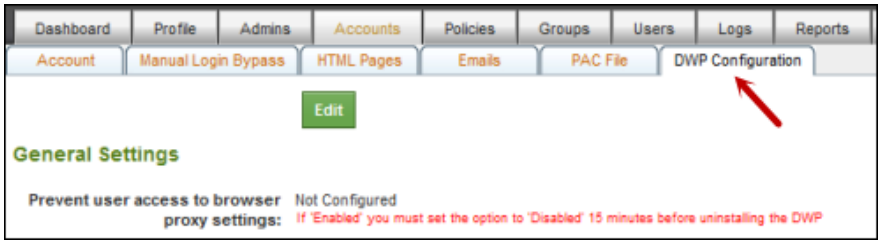
You can configure the Web Security Service to bypass web filtering for certain sites, such as internal intranets and trusted resources. If you want to bypass sites for your own requirements, follow the instructions in this section. Otherwise, you can skip this section.

Note: This procedure describes how to bypass web filtering at the account level. If you plan to use group-level settings, see the *Web Security Service Administrator Guide* or the *Management Portal Online Help*.

To bypass web filtering:

1. Select the **Accounts** tab and click **Edit**.

2. Select the **DWP Configuration** subtab.



3. Scroll down until you see the text box for: **Browser Bypass: Browser connects directly to the Internet**. (See the example on the next page.)

4. In the **Browser Bypass**... field, enter the sites stored in the browser's exception list.

   - Use a semicolon to separate the site entries.
   - Wildcard entries (*.*) are allowed.
   - You do *not* need to enter **http://** before each site name.

5. Click **Save**.
   It may take up to 15 minutes for the changes to take effect.

About Webroot

Webroot is bringing the power of software-as-a-service (SaaS) to Internet security with its suite of Webroot® SecureAnywhere™ offerings for consumers and businesses, as well as offering its security intelligence solutions to organizations that also focus on cyber-security, such as Palo Alto Networks, F5 Networks, Corero, Juniper, and others.

Founded in 1997 and headquartered in Broomfield Colorado, Webroot is the largest privately held Internet security organization based in the United States.

For more information on our products, services and security visit

- Our website: www.webroot.com
- Webroot Threat Blog: http://blog.webroot.com
- Webroot on Twitter: http://twitter.com/webroot

Webroot Headquarters
385 Interlocken Crescent,
Suite 800
Broomfield, Colorado 80021 USA

Tel: **+1 800 870 8102**

Webroot - APAC:
Level 14, Tower A,
821 Pacific Highway
Chatswood, NSW 2067 Australia

Tel: **+1 800 013 992**

Webroot - UK
Venture House, Arlington Square,
Downshire Way
Bracknell, England

Tel: **+44 (0) 800 804 7015**