Product Update Bulletin

Overview

This October’s console release adds many new features and capabilities to allow deeper policy control of your Webroot® DNS Protection service, and easier everyday management of our award-winning Webroot® Security Awareness Training. This release also includes the addition of API access and reporting to the business version of the management console.

As a reminder to all endpoint security Administrators, please ensure you have now enabled your endpoint protection Script Shield. This is an essential and very effective security protection and prevention component. In addition, for Mac deployments, we are pleased to announce support for Apple’s latest operating system version, macOS 11 (also known as Big Sur). It is fully supported with Webroot® Business Endpoint Protection agent version 9.1.3 and above.

Details on macOS agent upgrades to agent version 9.1.3 are here on the Business Community site, and details on enabling Script Shield are here.

Highlights in this release include:

Webroot® DNS Protection:

- DNS Privacy Policy Settings for DNS over HTTPS – You now have the ability to opt for complete user request privacy while preserving the essential DNS policy security filtering.

- Google SafeSearch Filtering – The Google SafeSearch Engine is now integrated into the Webroot DNS Service so it may be added as an extra filter to the existing URL categories.

- Enable Agent on Servers – The new default setting for running the DNS agent servers is now off, so for future deployments on servers, you will need to switch DNS on.

Webroot® Security Awareness Training:

- Auto-Enrollment – Administrators can now add new users automatically rather than duplicating or re-launching a campaign(s) to reach new users that have been added since a campaign was launched.

- Microsoft Azure AD Integration – Unlike older Azure AD integrations, Webroot’s SCIM-based integration is available to any organization subscribed to Microsoft 365 and does not require anything else to be installed. It also keeps users in the Webroot Security Awareness Training management console in sync with the AD tenant, so you no longer need to upload files or manually create users.

- New Training and Phishing Content – In the past quarter, over 15 new training modules added, including coverage of COVID scams and compliance courses on CCPA, GDPR, HIPAA and PCI. In addition, many new phishing templates and an easy-to-use template editor are now available.

API addition to the business version of the management console:

- API Access – Creating API client credentials allows you to connect with the Unity API system using a secure, authenticated connection between the Webroot® management console and your managed systems. This, in turn, allows you to automate billing, reporting, deployment and other processes.

- API Reporting – Using the Webroot Universal Reporter tool you can now create customized reports enabling you to save time and show real value from any data source.

- API Access and API Reporting – Both of these features are already available for users of the Managed Service Provider version of the management console.
New features in this release

1. Privacy Policy Settings

The new DNS Policy tab now offers Privacy Settings for DOH (DNS over HTTPS) requests, including the ability to opt for complete user request privacy while still preserving the essential DNS policy security filtering. The ideal setting for GDPR or other compliance standards.

![New DNS Privacy Policy Panel for DoH and DNS requests](image)

There are three Privacy Settings options now available:

i) **Hide User Information** – Selecting this option for a user or group of users turns off logging of all requests within a policy so user data such as “User” and “Domain” are not collected for any requests made either via the DNS Agent or at a network level. We do however retain data like IP address and Domain in case later troubleshooting is required. However, automatic DNS and DoH security filtering policy and any web URL category access restrictions are still enforced and applied to user or network requests.

![Selecting Privacy Setting - 'Hide User Information'](image)

ii) **Local Echo** – Selecting this option routes DNS and DoH requests to both the local DNS servers inside your network AND Webroot’s DNS service servers in the Google cloud. This allows DNS request data to be collected from your local DNS server(s) to provide request data for further analysis or to feed a SIM/SIEM/MDR/XDR security tool.

![Selecting Privacy Setting - 'Local Echo'](image)
iii) Fail Open – In the unlikely event that the Webroot DNS Protection service is unreachable and not able to process your requests, all DNS and DoH requests are automatically routed to your local DNS server(s) to resolve those requests instead of through Webroot.

2. Enabling Google SafeSearch

Google SafeSearch filtering is now integrated into the Webroot DNS Service so it is easily added to any existing filtering policy. As Google SafeSearch requests are filtered in our cloud, the SafeSearch engine filters are automatically applied to any request, regardless of source, if added to a policy. As a cloud policy, there is also no need to worry about the application generating requests, as the policy covers all requests without any further implementation work being needed.

3. Enable DNS Agent on Servers

By having the Webroot DNS Agent installed on all the Servers you run, you will get visibility by server name of all Internet requests made. However, on the wrong server this can cause conflict issues (an internal DNS server for instance) and the data will be rarely or ever used. To avoid any such conflicts in the future the default server setting in the Agent is disabled on Servers.

In the future, as an Administrator, you will have to consciously select the enabling of DNS agents on servers. Customers who already run the DNS Agent on their servers will not be affected by this change.
Webroot® Security Awareness Training:

The ability to create training campaigns that auto-enroll new users is a major time-saver for administrators. Combined with Microsoft Azure AD integration for importing users, this really helps you automate security awareness campaigns. Webroot also continues to introduce timely new training and phishing content every month. All of these features are now available on both our Managed Service Provider and business management consoles.

4. Microsoft Azure Integration – All Consoles

Microsoft Azure Active Directory (AD) integration keeps users in the Webroot Security Awareness Training console in sync with the AD tenant, so you don't need to upload CSV or LDIF files, or manually create users, although these options are available (if you require or prefer them). Azure integration helps automate the initial import of target trainees, as well as the future adding/removing of user trainees as they join or leave your organization. Webroot's SCIM-based integration is available to any organization subscribed to Microsoft 365 and does not require anything to be installed, making it much easier and faster to use and deploy. A video covering Webroot Security Awareness Training and Microsoft Azure AD integration is available here.

5. Auto-Enrollment

When creating a new training or phishing campaign, administrators now have the option to turn on a new Auto-Enrollment function. When selected, this will automatically enroll any new trainee users and ensure they receive that campaign's email communications automatically.

With this option enabled, administrators no longer have to duplicate or re-launch campaigns to reach new user trainees that have been employed or added since the campaign was originally launched.
6. New Training and Phishing Content

Since July we have added over 15 new training modules from NINJIO, including coverage of COVID scams and compliance courses on CCPA, GDPR, HIPAA and PCI. We have added new Webroot courses and considerably expanded the phishing email templates and lure pages based on real world attacks that impersonate popular online productivity and collaboration tools. We have also added a new template editor to make the tailoring of internal or personalized phishing templates very easy.

Overall, there are now nearly 100 training courses covering Security, Compliance, IT and Business Skills, plus over 200 up-to-date, real-world phishing examples. And all courses are now available when trialling Webroot Security Awareness Training too.

API Access and Reporting for the Business Management Console

Already available in our MSP (Managed Service Provider) Console, and now available in the business console, the Webroot API platform allows administrators to create their own applications (or enrich their existing applications) with data and functions provided directly from the Webroot cloud (for example, using API-extracted data to enrich reporting, or using the credentials in a supported Webroot RMM plugin for turning on advanced features).

By creating your own client credentials for authenticating against the API platform, leveraging the powerful console web API is only a small step away. Client credentials (i.e. a client identifier and client secret) are used to identify your application talking to the API platform. In addition, when authenticating with the API, users of your application specify their regular Webroot console login credentials to gain access to provided GSM and site management data and functions.

7. API Access

API Access can be found under the Settings section in the console.
8. API Reporting (Universal Reporter)

API Reporting can also be found under the Reports section in the console.

More information about API access and our Unity API may be found [here](https://www.webroot.com/us/en/business/customer-success). More details on Universal Reporter and reporting templates is [here](https://community.webroot.com/).

**To Close**

For many of our continuous minor releases, we do not issue Product Update Bulletins, however we do plan to start issuing a new monthly "What's New" update in the Business Community to keep you informed. In the meantime, there are many places where you can stay informed, or reach out to others for insightful advice and information.

Here are some useful resources:

- The Webroot Business Community is where to ask questions and get help and advice plus access to Knowledge Base articles: [https://community.webroot.com/](https://community.webroot.com/)