**http://www.techrepublic.com/blog/security/a-look-into-microsoft-security-essentials-2012/7058?tag=nl.e036**

**A look into Microsoft Security Essentials 2012**

By [Scott Lowe](http://www.techrepublic.com/search?q=scott+lowe)

Takeaway: Scott Lowe takes a detailed view into the Microsoft Security Essentials latest build, still in beta, noting some of the changes and performing some basic testing.

Last month, my TechRepublic colleague Mark Kaelin [announced](http://www.techrepublic.com/blog/window-on-windows/test-a-beta-version-of-microsoft-security-essentials/5423) Microsoft’s introduction of the latest [Microsoft Security Essentials](http://windows.microsoft.com/en-US/windows/products/security-essentials) (MSE) beta. As you probably know, MSE is Microsoft’s free virus scanner for Windows PCs, providing protection against malware, spyware, and rootkits. I, like Mark, feel that MSE is a great product and I also recommend it to everyone I know. The fact that it’s a free product certainly works in its favor! In this article, I’m going to dig a little deeper in this beta product and see what’s changed since the most recent production release.

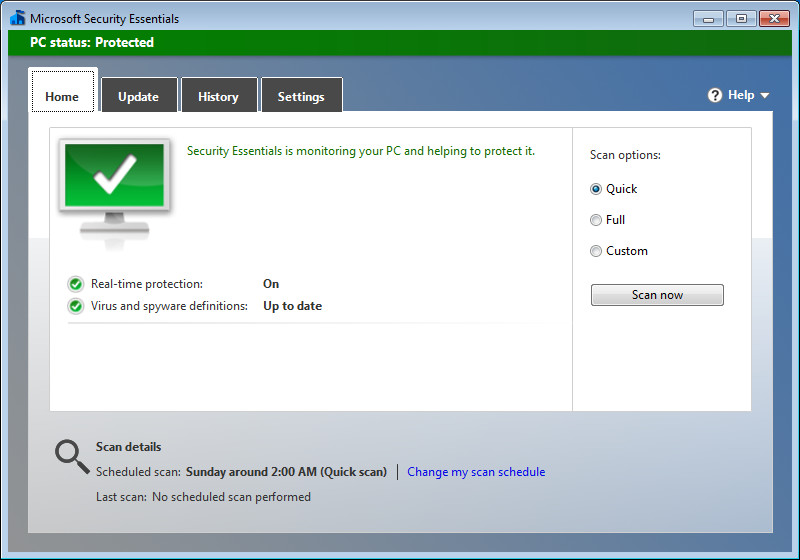
On my main PC in my lab, I have the latest current production release of MSE installed - build 2.1.1116.0. I will be looking at the beta that Microsoft recently announced, which carries a build number of 4.0.1111.0.

**The interface**

In some collateral material, Microsoft has indicated that the new MSE’s user interface has been streamlined, but I have seen little evidence of this in the latest beta. Given that this is a limited beta, it’s entirely possible that Microsoft has yet to implement the user interface enhancements. In **Figure A**, you can see that the beta MSE looks a whole lot like the old one with a couple of exceptions:

* The tabs in the old version also include small icons which are not included in this beta.
* The background color scheme has changed from gray with a “netting” image to a gray/blue blend.

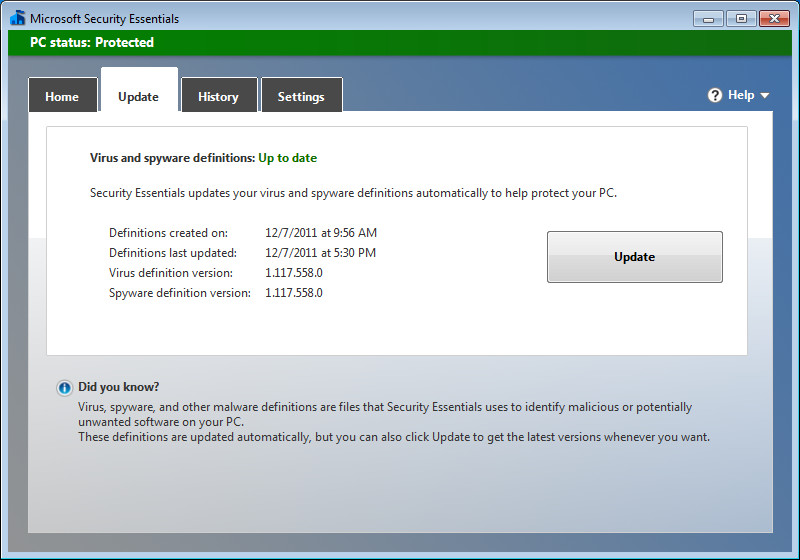
**Figure A**

[](http://i.techrepublic.com.com/blogs/a-mse.jpg)

**The new MSE looks a lot like the old MSE (click images to enlarge view)**

On the Update tab (**Figure B**), you can see that I downloaded the latest definitions soon after they were made available. Again, the page hasn’t changed at all since the older version that is currently in production.

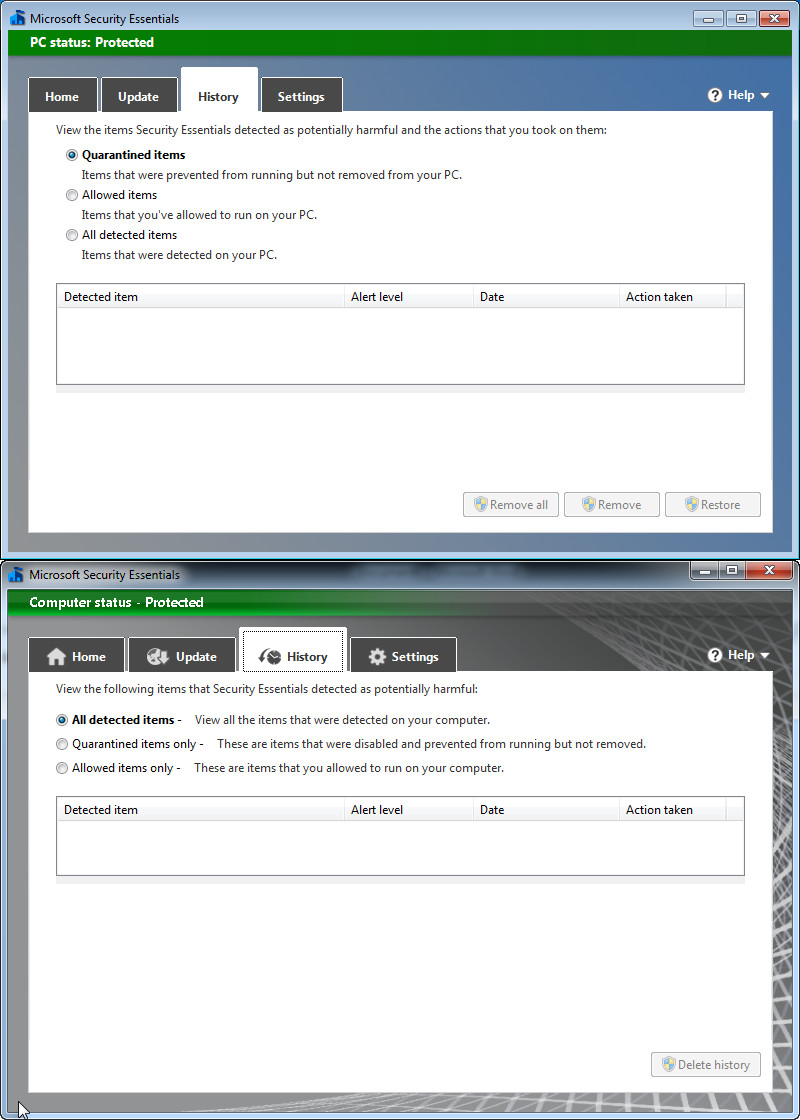
**Figure B**

[](http://i.techrepublic.com.com/blogs/b-mse.jpg)

**The MSE Updates page**

The most notable change to the interface that I’ve seen so far is shown in **Figure C** on which you can see the difference between the old History tab (Bottom) and the new one (Top). The primary difference is that some text has been rearranged, but little else has been changed.

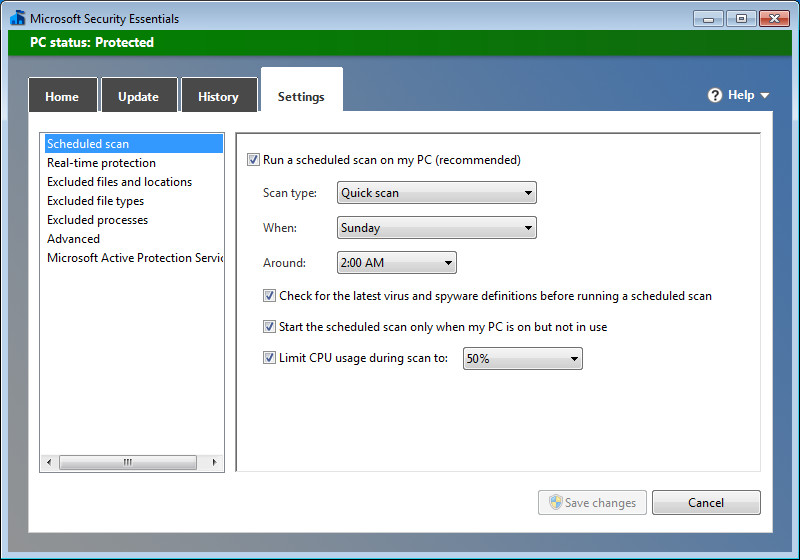
**Figure C**

[](http://i.techrepublic.com.com/blogs/c-mse.jpg)

**The MSE History page**

For the next few screenshots, I’ll be taking a look at the Settings tab. Again, not a lot has changed here except that this beta does not include an option for “Default settings”, which was present in the older MSE. In Figure D, you’ll see the Scheduled scan page from the new MSE. It’s identical to the old version. I ran through all of the drop-down menus as well and verified the lack of change. I’m not really surprised; there’s not much to change about a schedule!

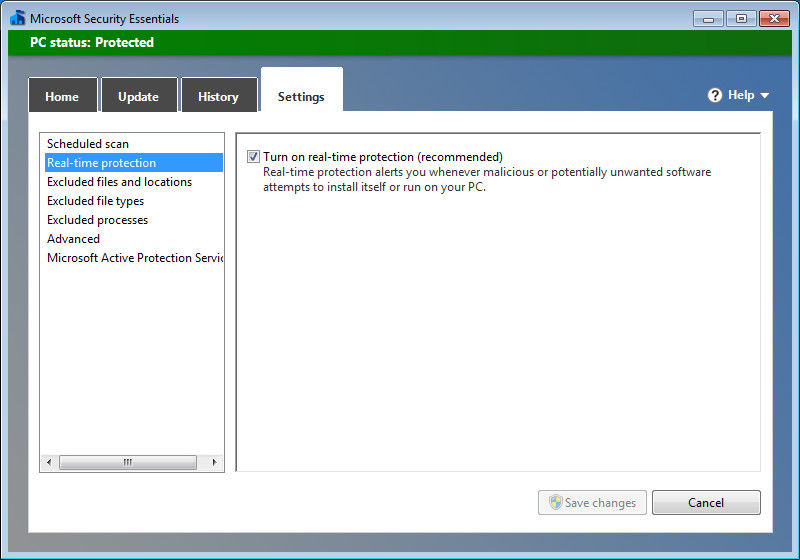
**Figure D**

[](http://i.techrepublic.com.com/blogs/d-mse.jpg)

**Settings for Schedule**

Here’s a screen that’s either been “streamlined” or that has yet to be completed in the beta. In **Figure E**, again, old on the bottom and new on top, the new version of MSE currently has much less in the way of options regarding real-time protection. In this beta, it’s all or nothing with regard to real-time protection.

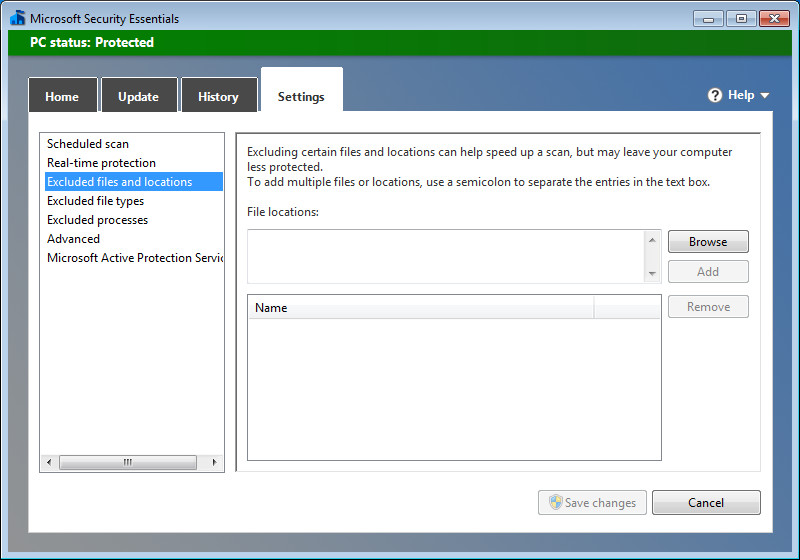
**Figure E**

[](http://i.techrepublic.com.com/blogs/e-mse.jpg)

**Real-time protection options in the MSE beta differ from the older version (for now)**

As has been the case for a while, MSE includes the ability to exclude certain files and locations from scanning. Some files contain what could be false positives and if they are quarantined or deleted, some applications could cease to function. You can see this screen in **figure F.**

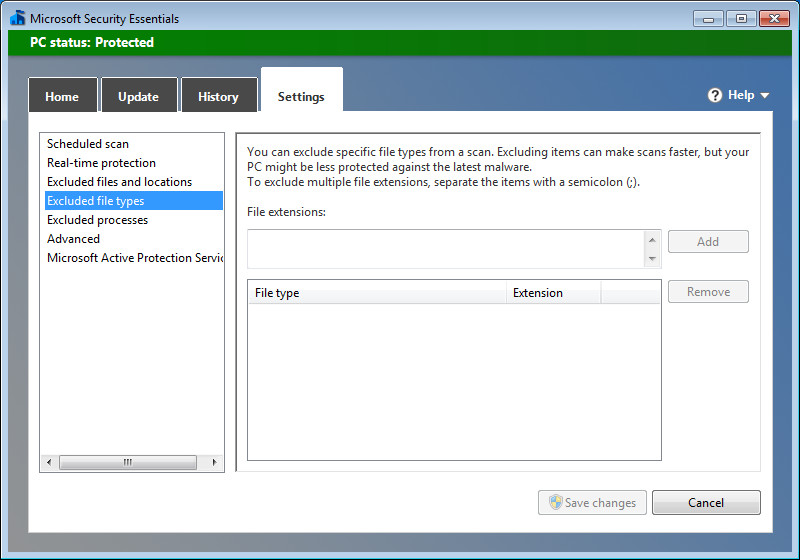
**Figure F**

[](http://i.techrepublic.com.com/blogs/f-mse.jpg)

**Exclude files and folders**

Likewise, you can also exclude files with specified extensions as shown in **Figure G**.

**Figure G**

[](http://i.techrepublic.com.com/blogs/g-mse.jpg)

**Exclude any file types that you wish**

Again, in **Figure H**, you’ll see another screen that hasn’t changed. This is the screen on which you can exclude specified processes from being scanned by MSE.

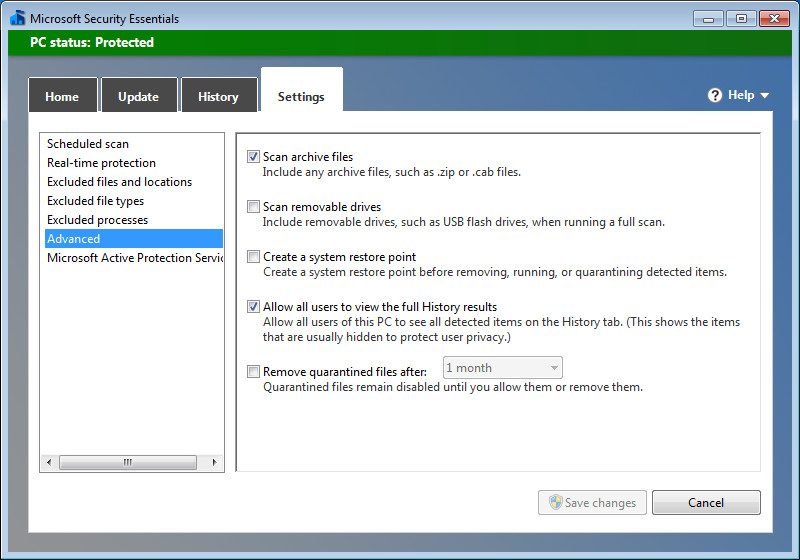
**Figure H**

[](http://i.techrepublic.com.com/blogs/h-mse.jpg)

**Exclude processes from scanning**

With the exception of some wording changes, the Advanced tab hasn’t changed a whole lot either. Here, you can decide how MSE should act when its running or when it’s discovered an infection. For example, you can configure MSE to create a restore point before doing anything with a detected item.

**Figure I**

[](http://i.techrepublic.com.com/blogs/i-mse.jpg)

**Configure MSE advanced options**

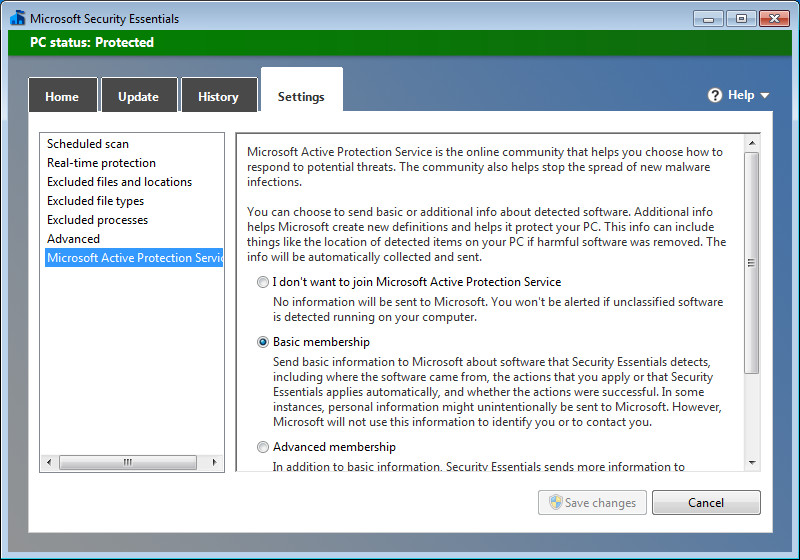
Finally, in **Figure J**, you’ll see that Microsoft has renamed SpyNet to Microsoft Active Protection Services. This is a service to which you can subscribe to help track your actions with regard to detected items. This is a community service that aggregates information from all subscribers in an attempt to help all make better decisions and better protect their systems.

You can choose not to participate or you can choose from two levels of membership:

* Basic. “Send basic information to Microsoft about software that Security Essentials detects, including where the software came from, the actions that you apply or that Security Essentials applies automatically, and whether the actions were successful. In some instances, personal information might unintentionally be sent to Microsoft. However, Microsoft will not use this information to identify you or to contact you.”
* Advanced. “In addition to basic information, Security Essentials sends more information to Microsoft about malicious software, spyware, and potentially unwanted software, including the location of the software, file names, how the software operates, and how it has impacted your computer. In some instances, personal information might unintentionally be sent to Microsoft; however, Microsoft will not use this information to identify you or contact you.”

Personally, I believe it’s important to participate in this service at some level.

**Figure J**

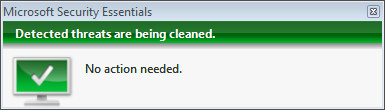
[](http://i.techrepublic.com.com/blogs/j-mse.jpg)

**The MSE Microsoft Active Protection Services screen**

**A little bit of testing**

As I said before, I’ve always liked MSE. It’s generally been fast, unobtrusive and complete. I tested the new MSE beta by visiting the [EICAR virus test site](http://www.eicar.org/86-0-Intended-use.html). I tried in a couple of different ways — both text and ZIP files via both HTTP and HTTPS and, as soon as I tried to download the EICAR test file, I immediately received a pop up message from MSE indicating that it had taken immediate action against the file and that no further action was required from the user.

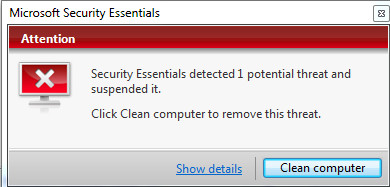
**Figure K**

[](http://i.techrepublic.com.com/blogs/k-popup.jpg)

**The MSE popup message**

This is an improvement from the older version of MSE, which stopped to ask the user for instructions (**Figure L**). One of Microsoft’s intents with the new version was to provide “Enhanced protection through automatic malware remediation: The Beta program will clean highly impacting malware infections automatically, with no required user interaction.” Based on this very limited testing, it’s obvious that they’re taking steps to deliver on this promise.

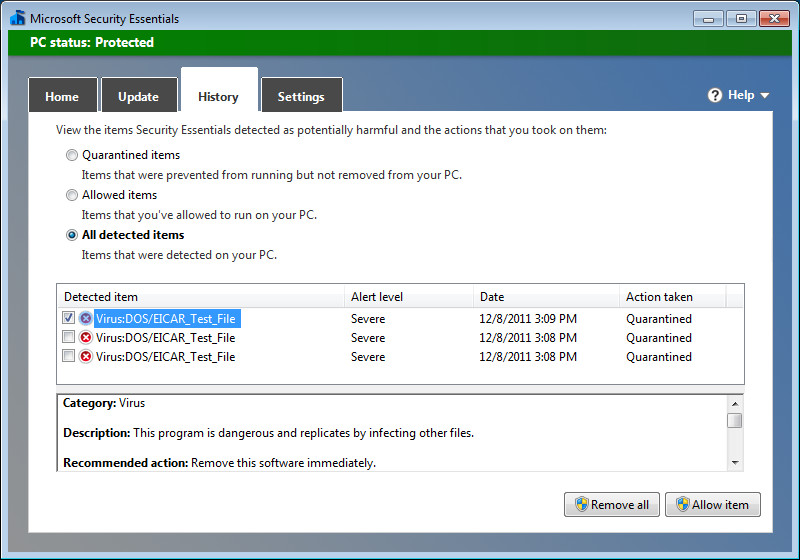
**Figure L**

[](http://i.techrepublic.com.com/blogs/l-old-popup.jpg)

**The same situation, but with the older MSE**

In reviewing the History information in MSE, you can see that the product did, in fact, see three separate instances of the EICAR test file (**Figure M**).

**Figure M**

[](http://i.techrepublic.com.com/blogs/l-history.jpg)

Microsoft has also indicated that the new MSE will have better performance and new detection capabilities. I haven’t been able to adequately test these promises, but MSE has always, for me, been snappy and very complete.