

Forefront Server Security Engine Revisions

Overview & FAQ

Published: July 2009

[Introduction 3](#_Toc233705720)

[Multiple Engine Protection 3](#_Toc233705721)

[Upcoming Engine Revisions 5](#_Toc233705722)

[Forefront Server Security and Antigen Service Pack Releases 5](#_Toc233705723)

[Forefront Server Security Engine Revision FAQ 7](#_Toc233705724)

# Introduction

The purpose of this document is to inform customers and partners about Microsoft engine strategy and changes beginning Dec. 1, 2009. This document provides an Overview and FAQ so that Forefront customers are aware of upcoming engine changes and able to address their antimalware engine configurations accordingly.

# Multiple Engine Protection

Implementing Forefront server security products enables organizations to function more efficiently by removing security threats associated with unwanted and malicious content entering organizations via e-mail, IM streams, and documents posted on SharePoint document libraries. These products incorporate a multi-engine strategy, including the use of Microsoft and industry-leading security partner technology, to consistently drive high detection rates.

As part of this multiple engine functionality, Forefront server security products include an advanced multiple engine manager that allows customers to concurrently configure up to five engines. Using multiple scanning engines delivers several critical advantages:

* It increases the chances that emerging threats will be caught quickly.
* It provides redundancy to help protect against scan failures or defects in individual engines; if an engine fails, other engines continue scanning messages.
* It gives administrators an effective way to choose the most appropriate level of protection for their environment given their security needs and server performance capabilities.
* It allows engines to be taken offline for updates or reconfiguration without forcing messages or documents to be queued.

Tests performed quarterly by the independent [AV-Test.org](http://www.av-test.org/) group have shown that the multi-engine set for Forefront security products rates highest in response times for “in the wild” viruses and variants.



* The above chart outlines recent test results conducted by AV-Test.org. Lab response times were tested for 365 “In the Wild” viruses and variants that appeared from January – March 2009 including testing the Forefront multi-engine set vs. three single-engine vendors.
* Test Results
	+ 203 viruses were proactively detected by all labs
	+ 162 viruses showed significant variations in detection times.
	+ The Forefront multi-engine set performed much better when compared to three leading vendors tested. Forefront multi-engine set had an average detection time of 6 hours for this three month period. The vendor solutions had average detection times of 26 hours, 83 hours and 206 hours, respectively.

# Upcoming Engine Revisions

Microsoft continually conducts extensive research, development and testing on third-party (vendor) antimalware engines included in its Forefront server security products to maintain and improve overall protection from malware. In addition to the technology benefits realized, we continue to build stronger technology relationships with our engine vendors that are a critical component of our multi-engine strategy and make investments in other areas, including antispam partnerships that will increase overall protection for our customers.

As noted previously, Forefront server security customers are able to concurrently configure up to five engines. We have found that having multiple engines consistently provides the highest detection rates against the competition with average response time of ***3-6 hours*** for new viruses. This is due to the management and amalgamation of unique engine characteristics including architecture, signature update/distribution frequency, heuristics and local and global presence. In contrast, competitive single-engine solutions average response times are more than ***2-9 days*** as noted in recent AV-Test.org data. In order to further develop stronger technology relationships with our antimalware partners and ensure continued customer value for the longer term, we are standardizing on a set of five antimalware engines moving forward, with confidence that this solution will continue to provide equal or better detection rates and response times than the industry’s other leading solutions.

What does this mean for Microsoft and its customers? The current and next generation of Forefront server security products, including Antigen, will include five antimalware engines as part of an ongoing strategy to maximize and maintain our malware detection advantages as well as make investments in other areas that will increase overall protection for our customers. As an example of our commitment to continual improvement of our malware detection leadership, we are investing in new antispam technology through a partnership with [Cloudmark](http://www.cloudmark.com/releases/docs/ds_cse_0309.pdf) that will provide an overall better antispam experience including higher detection rates, lower false positives, improved submission experience and enhanced service experience. Customers will be able to take advantage of these new enhancements and engine changes after deploying the Antigen and Forefront service packs released on July 1, 2009. (Cloudmark integration will be included in Antigen 9.0 Service Packs and the next generation release of Forefront Security for Exchange Server, due out later this year).

# Forefront Server Security and Antigen Service Pack Releases

Microsoft is providing visibility of new engine availability and engine retirement into the Forefront server security and Antigen products through the release of several new service packs. These service packs will allow customers to move to the new set of five engines as well as additional engine changes that Microsoft may release after December 1, 2009. The new features provided in each service pack are outlined below:

**Forefront Security for Exchange Server with Service Pack 2**

* Visibility of all actively published engines[[1]](#footnote-1)
* UI display of all available engines as well as currently configured engines
* Event logs and notifications provide information about new engine availability or retirement
* Rollup of software fixes

**Forefront Security for SharePoint with Service Pack 3**

* Visibility of all actively published engines[[2]](#footnote-2)
* UI display of all available engines as well as currently configured engines
* Event logs and notifications provide information about new engine availability or retirement
* Rollup of software fixes

**Antigen for Exchange with Antigen Spam Manager 9.0 with Service Pack 2**

* Visibility of all actively published engines[[3]](#footnote-3)
* UI display of all available engines as well as currently configured engines
* Event logs and notifications provide information about new engine availability
* Integration of leading anti-spam engine from Cloudmark.
* Rollup of software fixes

**Antigen for SMTP Gateways with Antigen Spam Manager 9.0 with Service Pack 2**

* Visibility of all actively published engines[[4]](#footnote-4)
* UI display of all available engines as well as currently configured engines
* Event logs and notifications provide information about new engine availability
* Integration of leading anti-spam engine from Cloudmark.
* Rollup of software fixes

**Antigen 8 for Exchange, SharePoint and IM**

* An update will be made available later in 2009 that will allow for the configuration of the new engine set.
* Customers who obtain Antigen 8 products from sybari.com may use the license configurator to generate a new license.cfg file based on the new engine set.

**Forefront Security for Office Communications Server**

* An update will be made available later in 2009 that will allow for the configuration of the new engine set.

# Forefront Server Security Engine Revision FAQ

**What five engines will be part of the new engine set effective December 1, 2009?**

Microsoft continually checks antivirus engine quality and detection rates through 3rd party independent testing organizations. We have found that using multiple malware engines consistently provides the highest detection rates against the competition and represents an average response time of 3-6 *hours* for new viruses. In contrast, competitive single-engine solutions average response times are more than 2-9 *days* as noted in recent AV-Test.org data. The set of five engines available in Forefront server security products as of Dec. 1, 2009 includes Microsoft AV, Kaspersky, Norman, VirusBuster and Authentium. However, these engines may change over time as we seek to improve overall protection metrics and to maintain our detection advantage relative to our competition and in support of our customer needs.

**Why is Microsoft eliminating some antimalware engines? Why did you decide on five?**

Microsoft continually checks antivirus engine quality and detection rates using internal and 3rd party independent testing organizations. We have found that having multiple malware engines consistently provides the highest detection rates against the competition and represents an average response time of 3-6 *hours* for new viruses. In contrast, competitive single-engine solutions average response times are more than 2-9 *days* as noted in recent AV-Test.org data. Testing for the last several years has indicated that using more than five malware engines concurrently does not improve overall detection rates. In order to develop stronger technical relationships with our antimalware partners and ensure continued customer value for the longer term, we are making available a new set of five antimalware engines, with confidence that this solution will continue to have the best catch rate and response times in the industry.

**Will the next generation Forefront server security products only have five engines?**

We have found that having multiple antimalware engines consistently provides the highest detection rates against the competition and represents an average response time of 3-6 *hours* for new viruses. In contrast, competitive single-engine solutions average response times are more than 2-9 *days* as noted in recent AV-Test.org data. Also, we have found that having more than five engines running concurrently does not really improve overall detection rates. In order to promote a stronger technical relationship with our antimalware engine partners and ensure continued customer value for the longer term, we are making available a new set of five antimalware engines for all Forefront server security products, including the next generation releases. Microsoft recommends Antigen and Forefront server security customers install and deploy the latest service packs by December 1, 2009 in order to take advantage of the new engine set. The next generation Forefront server security products will also include this feature.

**If you are only making available five antimalware engines, will the cost of Forefront server security products drop?**

We believe that the multiple engine detection provided in Forefront server security products offers significant value to our customers and this has not been reduced with this change. Although the total number of antimalware engines included in our products is changing, the overall value of our products is not and therefore the cost will not drop. We remain committed to providing the same leading detection and response time advantages our customers receive today. Customers will also benefit moving forward as we invest in new technology partnerships and deliver additional value around areas such as antispam.

**Why is Microsoft Forefront shifting to fewer engines?**

Forefront server security products provide a premium antimalware solution that uses multiple engines for rapid detection. As part of maintaining our high level of detection, Microsoft may make changes to the antimalware engine set. This gives us the flexibility to make necessary adjustments to the antimalware engine mix for maintaining and even improving our detection capabilities over time and also allows us to invest in other areas, such as antispam partnerships, where our customers have told us they would like to see additional functionality. Our customers should expect and continue to see the high detection levels offered by Forefront in their existing deployments. The highest priority for our business is to provide comprehensive protection for our customers, and we plan to continue our leadership in server workload protection.

**When is this move to five malware engines happening for all Forefront server security products?**

Forefront Security for Office Communications Server has already launched with five engines available. Microsoft recommends for Antigen and Forefront server security customers to deploy the new service packs available on July 1, 2009 prior to December 1, 2009, when several existing engines will be retired.. After December 1, 2009, the new set of five engines will be the engines that continue to receive signature updates.

**Do I need to install the service pack by December 1, 2009 in order to continue receiving signature updates?**

No, it is not required. However, the service pack will provide you with notifications of further engine changes and automatically make available new engines to you. If you have an existing contract for product shipping with eight engines, you will continue to have support for the existing eight engines available through December 1, 2009. After this date, signature updates will not be provided for retired engines. To take advantage of the new set of five engines, it is recommended that you deploy the appropriate product service pack before December 1, 2009.

**How will I be informed of engine changes after deploying my Antigen/Forefront service pack?**

For the engines being retired, an announcement is written to the event log to inform customers regarding the date on which updates for this engine will no longer be available. You can also configure notifications to be sent to **Virus Administrators** in addition to the event log. Notifications including links to information about engine retirement are written to the event log on a weekly basis. One month before the date the engine is scheduled to be retired, the event log notifications are written on a daily basis. This will allow you to take action and reconfigure your engine set.

For engines being added, an announcement is written to the event log that publicizes that the engine was added to your configuration. You can also configure notifications to be sent to **Virus Administrators** in addition to the event log. This notification, which includes links to information about this new engine, is written to the event log only once. Once notified, you will have ability to enable the new engine as part of your security configuration.

**If I configure my engine set to the new set of five engines, will I no longer be able to use the other engines before December 1, 2009?**

If you have an existing contract for product shipping with eight engines, you will continue to have support for eight engines through December 1, 2009. All eight engines will be available through that time for you to configure as needed for your environment. After December 1, 2009, only the new set of five engines will be available for configuration.

**What is Microsoft’s recommendation on when to reconfigure the engine set to the new five engines?**

Customers with an existing contract for product shipping with eight engines will continue to have support for eight engines through December 1, 2009. While not required to deploy the service pack, in order to take advantage of the new set of five engines, it is recommended that customers deploy the appropriate service pack before December 1, 2009.

**What happens if I don’t deploy the service pack prior to Dec. 1, 2009?**

Customers will continue to receive updates for engines included in the new engine set regardless of whether or not they have installed the service pack release. However, they will not receive any updates for retired engines. This means that customers who do not deploy the service pack will have to manually deselect any retired engines they are using and replace them with available engines from the new engine set. Also customers who do not install the service pack will not have access to any new engine that Microsoft releases after Dec. 1, 2009. Therefore, we highly recommend all customers install the service pack prior to Dec. 1, 2009.

For Antigen 9.0 customers, we recommend that you deploy the service pack as early as possible to take advantage of new antispam enhancements. While the Mailfilters SpamCure antispam engine will be available to you through December 1, 2009, we highly recommend you configure Cloudmark as your antispam engine as early as possible.

**After deploying Antigen 9.0 with SP2, I am seeing both SpamCure and Cloudmark antispam engines listed in the UI? Which one does Microsoft recommend I use?**

As an example of Microsoft’s commitment to continual improvement of our malware detection leadership, we are investing in new antispam technology through a partnership with Cloudmark that will provide an overall better antispam experience including higher detection rates, lower false positives, and improved submission and service experience. The Cloudmark engine with Antigen 9 is being released as Beta with the July 1, 2009 service pack as it is currently in customer trials. Upon completion of the customer trials it will be released and you will be able to find updated information on the AMEND TechNet page.

The Mailfilters SpamCure antispam engine will be available in Antigen 9 through December 1, 2009. We highly recommend that our customers switch to the Cloudmark engine as early as possible in order to benefit from the antispam enhancements. As of December 1, 2009, we will no longer license nor provide updates to the MailFilters engine. Therefore, to continue antispam coverage, the Cloudmark engine will need to be configured as the antispam engine prior to December 1, 2009.

**I have an existing Antigen 9/FSE/FSSP deployment. Will I lose support for some of my engines?**

If you have an existing contract for product shipping with eight engines, you will continue to have support for eight engines through December 1, 2009. To take advantage of the new set of five engines, it is recommended that you deploy the appropriate product service pack before December 1, 2009.

1. The current Forefront server security product version does not provide visibility on when a new engine becomes available or on when an engine is being retired.  Deploying the service pack provides that guidance and allows for a new engine to be configured without having to do any product upgrade. [↑](#footnote-ref-1)
2. The current Forefront server security product version does not provide visibility on when a new engine becomes available or on when an engine is being retired.  Deploying the service pack provides that guidance and allows for a new engine to be configured without having to do any product upgrade. [↑](#footnote-ref-2)
3. The current Forefront server security product version does not provide visibility on when a new engine becomes available or on when an engine is being retired.  Deploying the service pack provides that guidance and allows for a new engine to be configured without having to do any product upgrade. [↑](#footnote-ref-3)
4. The current Forefront server security product version does not provide visibility on when a new engine becomes available or on when an engine is being retired.  Deploying the service pack provides that guidance and allows for a new engine to be configured without having to do any product upgrade. [↑](#footnote-ref-4)