Anti-virus options

ANTI-VIRUS OVERVIEW .................................................................................................................. 2
ENVIRONMENTS IN WHICH THE ANTI-VIRUS PRODUCTS CAN BE USED ........................................... 2

MANAGED ANTI-VIRUS ENVIRONMENTS .................................................................................................. 3
What does it mean to have a computer in the Managed environment? .................................................. 3
What criteria needs to be met to have a machine in a Managed” environment? ............................... 3
In the Managed environment, how does Forefront get installed on a computer? .............................. 3
Once FCS has been installed, what needs to be done to the computer? .............................................. 3

Fully Managed ...................................................................................................................................... 4
What specifically does it mean to be in a FCS Fully Managed Environment? ........................................ 4
How exactly does a computer in a FMC receive their updates? ............................................................ 4
What steps are necessary for a machine to become Fully-Managed? .................................................. 4
If I receive an update, will my computer automatically reboot? ............................................................ 4
How often will virus scans take place? ................................................................................................... 4
Which patches are downloaded in the fully managed environments? .................................................. 5

Semi-Managed ..................................................................................................................................... 6
What specifically does it mean to be in a FCS Semi- Managed Environment? .................................... 6
What is necessary for a machine to become Semi-Managed? .............................................................. 6

UN-MANAGED (AKA MICROSOFT SECURITY ESSENTIALS (MSE)) .................................................................... 7
What specifically does it mean to be in an “Un-Managed” Environment? ........................................ 7
How does MSE differ from FCS? ........................................................................................................... 7
How to install MSE? ............................................................................................................................. 7

APPENDIX A: COMPARISON OF FCS 2.0 AND MSE ............................................................................. 8
APPENDIX B: FORCING AN IMMEDIATE INSTALLATION OF FCS 2.0 AND SIGNATURES ......................... 9
After FCS is installed is there anything else that needs to be done? .................................................... 9

APPENDIX C: McAFFEE REMOVAL ..................................................................................................... 10
APPENDIX D: MSE INSTALLATION: .................................................................................................... 12
APPENDIX E: AVAILABLE AUTOMATION ......................................................................................... 13
APPENDIX F: CONVERSION CHECKLIST: .......................................................................................... 14
Anti-Virus Overview

To ensure that OSU faculty/staff and students have access to software to protect their computers and OSU network from viruses, OSU provides two options. The available options are Microsoft Security Essentials (MSE) and Microsoft Forefront Client Security (FCS). Appendix A: shows how both products are virtually identical with the exception of the network management functions available in FCS.

*Note: Forefront and Essentials only apply to Windows based Machines. Individuals on the Macintosh platform can continue to use McAfee until a suitable replacement has been found.

**Note: Forefront should not be installed on Laptop computers. Laptops should have MSE installed.

Environments in which the anti-virus products can be used

There are three environments in which these anti-virus products can be used.

<table>
<thead>
<tr>
<th>Environment</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully-Managed</td>
<td>In the fully managed environment, the computer would be part of the ad.okstate.edu Active Directory domain. The computer would place in an “FCS_Managed” container set up for the college, department or campus. Computers located in this container will automatically have the client installed during a Microsoft Update. In addition virus signatures, updates, Microsoft service packs, updates, and patches, etc. will be handled centrally.</td>
</tr>
<tr>
<td>Semi-Managed</td>
<td>In the semi-managed environment, the computer would be part of the ad.okstate.edu Active Directory domain. However, the computer would NOT be in the “FCS Managed” container. The Forefront client would need to be installed on each computer individually and configured individually. Note: The Forefront client would be pre-configured for central reporting.</td>
</tr>
<tr>
<td>Un-Managed</td>
<td>In the un-managed environment, the computer could or could not be in the ad.okstate.edu Active Directory domain. Microsoft Security Essentials would need to be installed and configured on each computer individually. Central reporting is not available.</td>
</tr>
</tbody>
</table>
Managed anti-virus environments

What does it mean to have a computer in the Managed environment?
Computers in the Managed environments would report to a central reporting server managed by IT. IT Security Office and IT Server Administration monitor the alerts to determine if a computer is infected. If a computer is infected, notification via a Help ticket will be sent to the ITC for the department, college or campus. Overtime, individual reports by department, college or campus will be provided. The reporting server also provides information on the types of viruses stopped. This provides valuable information for IT Security on securing the infrastructure against possible threats.

In a Fully-Managed environment, the computer will also receive all security updates and virus/malware signature files from the FCS environment. In the event the FCS environment is unavailable, the fallback is to use the Microsoft servers. This architecture change will free bandwidth to the Internet.

What criteria needs to be met to have a machine in a Managed” environment?
1) The computer is Windows based.
2) The computer needs to be a member of the ad.okstate.edu Active Directory domain.
3) Forefront needs to be installed on the computer.
4) The computer should not be a laptop.
5) Port TCP 80 and TCP/UDP 1270 need to open on the computer firewall

In the Managed environment,how does Forefront get installed on a computer?
There are two ways in which Forefront can get installed on a machine a managed environment.

The first way is to move the machine into the fully managed container (see Fully Managed below). Once this occurs, Forefront will be downloaded via Microsoft Updates within 24hrs. Once the program has been downloaded, Microsoft Updates can be run. If there are no programs running which prevent the FCS application from being installed, FCS will install. At that point, the signature files will be downloaded and applied to the computer within 24hrs.

The second way is to force a Forefront installation on the computer. See Appendix B:

Once FCS has been installed, what needs to be done to the computer?
After FCS is installed and the signature files have been installed, it will be necessary to remove McAfee from the computer. See Appendix C:
Fully Managed

What specifically does it mean to be in a FCS Fully Managed Environment?
In the fully managed environment, a “FCS_Managed” container (FMC) will be located within the “Workstations” container for the college or campus. Computers placed in this container would then be considered fully managed. An example of the directory structure is shown below:

How exactly does a computer in a FMC receive their updates?
The MS Forefront install file is delivered to the computer through Microsoft Updates.

What steps are necessary for a machine to become Fully-Managed?
The computer must be placed in the FCS_Managed container; FCS needs to be installed; and ports TCP 80 and TCP/UDP 1270 need to be open on the computer’s firewall.

If I receive an update, will my computer automatically reboot?
No. The update must be approved on each individual’s computer before a reboot. When installing patches, updates, etc., the computers will not, “self-reboot”. The reboot will only take place upon user approval.

How often will virus scans take place?
A full virus scan will take place once a week. A quick scan will take place every 7 hours. Note: If the full scan is skipped twice, FCS will force a full scan the next time the computer is rebooted.
Which patches are downloaded in the fully managed environments?

Microsoft Products

Forefront

Office 2003
Office 2007

Silverlight

SQL Server

Silverlight

SQL Server 2005
SQL Server 2008

Windows

Windows 7
Windows Internet Explore 7 Dynamic Installer
Windows Internet Explore 8 Dynamic Installer
Windows Media Dynamic Installer
Windows 2003
Windows 2008 R2
Windows Server 2008 Server Manager Dynamic Installer
Windows Server 2008
Windows Server Manager - Windows Server Update Services
Windows Vista Dynamic Installer
Windows Vista
Windows XP
Semi-Managed

What specifically does it mean to be in a FCS Semi-Managed Environment?
In the semi-managed environment, the computer would be part of the ad.okstate.edu Active Directory domain. However, the computer would NOT be in the “FCS_Managed” container (FMC). The Forefront client would need to be installed and configured on each computer individually.

Note: The Forefront client would be pre-configured for central reporting.

What is necessary for a machine to become Semi-Managed?
1) The computer must be in the ad.okstate.edu AD directory.
2) Forefront must be installed on the computer.
3) Ports TCP 80 and TCP/UDP 1270 need to be open on the computer’s firewall.
Un-Managed (aka Microsoft Security Essentials (MSE))

What specifically does it mean to be in an “Un-Managed” Environment?
The Un-Managed environment is the default security environment provided by Microsoft. This is the preferred environment for laptops, personal computers. This will be the only option available for students.

How does MSE differ from FCS?
There is not really much of a difference at all. Appendix A: highlights the key differences. For the most part the only difference is the MSE does not provide the reporting capabilities that FCS does.

How to install MSE?
Appendix D: MSE Installation:
Appendix A: Comparison of FCS 2.0 and MSE

<table>
<thead>
<tr>
<th>Feature</th>
<th>Forefront Client Security</th>
<th>Microsoft Security Essentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus/AntiSpyware</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rootkit Protection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Win 7 &amp; WS 2008 R2 Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Dynamic Signature Service</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Group Policy Control</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Centralized Management &amp; Reporting</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Integrated Host Firewall Management</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Security State Assessments &amp; Remediation</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>NAP Integration</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>External Device Control</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Automatic Endpoint Discovery</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Appendix B: Forcing an immediate installation of FCS 2.0 and Signatures

The Forefront Client can be installed by using the batch file FCSInstall located at: \stwfile01.ad.okstate.edu\AV\FCSBatchInstall\.

The FCSInstall will install the Forefront Client with the appropriate configuration settings for centralized reporting. However, it will NOT apply the most recent virus signature files.

Are there some products which could prevent FCS from installing correctly?
Yes. Currently we know the following products have caused FCS to not install:
1) Microsoft One Care
2) Microsoft Defender
3) Microsoft Security Essentials
4) Spyware doctor 2005

After FCS is installed is there anything else that needs to be done?
Once FCS has been installed, it is critical to ensure that the FCS Signatures are also applied and are up to date. The process for doing is been described by Microsoft in the following KB entry:

http://support.microsoft.com/?id=935934
Appendix C: McAfee Removal

McAfee provides a link describing how to remove their products at:

McAfee provides a tool to remove its products at
http://download.mcafee.com/products/licensed/cust_support_patches/MCPR.exe

Please be aware:
1) This application must be run as an Administrator.
2) The McAfee removal tool fails when Access Protection Control is on. Therefore, Access Protection Control MUST be turned off before executing this application.

To disable Access Protection Control:
1) Log into the Windows operating system as an Administrator.
2) In the System Tray (near the clock), right click McAfee and select Virus Scan Console from the list.
3) A new window titled Virus Scan Console should appear. Right click the Access Protection item in the list and select Disable from the menu.

**Note: There have been reports that even with Access Protection disabled, the McAfee removal tool fails.
McAfee Removal:
These steps are “time-sensitive”, due to the nature of the ePolicy Orchestrator Client. **If you are running Lotus Notes, please close it before proceeding.**

1. To begin, open a cmd.exe window (if in Windows Vista, ensure you are running cmd.exe as an Administrator). Verify that you are on the C: drive, if not, then type c: (and press enter)

2. Then type:
   
   cd “\program files\mcafee\common framework\” (and press enter)
   
   or
   
   cd “\program files\network associates\common framework\” (and press enter)
   
   (Only one of these two directories should exist on most ePO managed installations.)

   i. If you encounter a “too many parameters” error when attempting Step 2, type:
      
      cd progra~1\mcafee\common~1 (and press enter)
      
      or
      
      cd progra~1\networ~1\common~1 (and press enter)

3. Leave the cmd.exe window open; it will be returned to shortly.

4. Right-click on the McAfee shield in the bottom right-hand corner of the screen (the tray)

5. Select “VirusScan Console” from the list.


7. On the “Access Protection Properties”, uncheck “Enable Access Protection” and “Prevent McAfee services from being stopped”, then click Apply and then OK.

8. At the command prompt previously opened, type `frminst /remove=Agent` (and press enter). This will launch the McAfee Updater, and after a short time will remove the ePO agent.

   i. If you encounter a 1704 error message, click Yes.

9. Remove McAfee VirusScan Enterprise

   i. Typically, this is done in Add/Remove Programs. If it is not listed in Add/Remove Programs, but is still in the system tray, then an MSIEXEC command can be run to remove it, depending on the version of McAfee installed (right-click the VSE icon in the system tray and select “About VirusScan Enterprise). **If you must use the MSIEXEC method, this will require a reboot. Save any work in progress before proceeding.**

   For VirusScan Enterprise 8.7i
   
   msiexec.exe /x {147BCE03-C0F1-4C9F-8157-6A89B6D2D973} REMOVE=ALL REBOOT=R

   For VirusScan Enterprise 8.5i
   
   msiexec.exe/x {35C03C04-3F1F-42C2-A989-A757EE691F65} REMOVE=ALL REBOOT=R

   For VirusScan Enterprise 8.0i
   
   msiexec.exe /x {5DF3D1BB-894E-4DCD-8275-159AC9829B43} REMOVE=ALL REBOOT=R

10. Remove “McAfee Agent” from Add/Remove Programs (if it exists) and restart your computer. Otherwise, restart your computer.
Appendix D: MSE Installation:

Microsoft has provided extensive documentation on the Security Essentials software, including instructions on how to download, install, and set-up the software. For information on how to download, install, and update MSE visit the support page Microsoft Security Essentials URL: (http://www.microsoft.com/security_essentials/default.aspx?mkt=en-us#dlbutton)

The support page for the installation of this software contains How-To videos. The “Help and How-To” page contains Top Support topics, general questions, and options for more help and How-To’s.

Additional useful information can be found at: http://www.malwarehelp.org/
Appendix E: Available Automation:

Installation:
Information Technology (IT) provides an application to ensure the most efficient and least intrusive change over to FCS or MSE from McAfee.

The application will be able to detect if the computer is in the ad.okstate.edu Active Directory domain (or not); and which version of MacAfee is running.

This application will ensure Forefront is correctly installed on the computer and will automatically remove McAfee. While executing, if the application encounters any errors, a message will be displayed along with instructions on how to resolve the error encountered and exit.

The application is designed to be run multiple times on the same computer with no adverse effects. Based on the information gathered from the computer, it will continue to step through the process. The application will notify the customer when the computer has FCS successfully installed and McAfee is uninstalled.

The application named OSU-AV will be located at:
`\stwfile01.ad.okstate.edu\AV\OSU-AV\`

*Note to ITC’s:  We are happy to provide the source code upon request.
** Note the applications OSU-AV is scheduled to be made available in mid March.

Reporting:
IT is working to provide a report to the ITC’s of all the machines in their containers to show if Forefront, McAfee or both are running. This report is intended to assist in easily determining if a machine needs to have Forefront Installed and McAfee removed.

Note: For this report to be generated each machine needs to have the Domain Administrators group in the Local Administrators group on the computer being checked.
**Appendix F: Conversion Checklist:**

IT would like to coordinate the conversion with you. To ensure a smooth transition from McAfee an IT technician can be scheduled to assist in getting started with the conversion. Technicians will be available beginning in mid-March.

Please return the following checklist via a help ticket to IT.

<table>
<thead>
<tr>
<th>Checklist</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Best contact phone #</td>
<td></td>
</tr>
<tr>
<td>Number of Mac Workstations?</td>
<td></td>
</tr>
<tr>
<td>(needed for McAfee Licensing renewals)</td>
<td></td>
</tr>
<tr>
<td>Where to locate your Fully Managed Containers?</td>
<td></td>
</tr>
<tr>
<td>Date when you plan on beginning your conversion.</td>
<td></td>
</tr>
<tr>
<td>Where would you like tickets routed if an infected workstation is detected?</td>
<td></td>
</tr>
</tbody>
</table>