

IT Security Products for Small Business



Review of IT Security Suites for Small Business, 2014

Language: English

October 2014

Last revision date: 22nd October 2014

www.av-comparatives.org

Contents



- About this review3
- Products reviewed.....5
- AV-Comparatives Approved Business Product Award 20146
- Management Summary.....7
- Product reviews9
 - Avira Endpoint Security.....9
 - Bitdefender Small Office Security (cloud)..... 16
 - ESET Endpoint Security 22
 - F-Secure Protection Service for Business..... 28
 - G Data Antivirus Business..... 35
 - IKARUS security.manager 41
 - Kaspersky Small Office Security 45
 - McAfee Endpoint Security (Self-Managed Option)..... 52
 - Sophos Endpoint Security and Control with Sophos Cloud..... 60
 - Symantec Endpoint Protection Small Business Edition 66
- Feature lists.....73

About this review

AV-Comparatives' 2014 small-business software review looks at security products suitable for a company running either the Foundation or the Enterprise edition of Microsoft Windows Server 2012 R2. As can be seen on the Microsoft Website¹, the Foundation version is suitable for small companies with up to 15 users, while the Essentials version allows an additional ten users. The report thus considers products for a network of up to 25 client PCs, with one file server/domain controller.

As Windows XP is no longer supported by Microsoft, and relatively few Windows Vista systems are in use, we have used Windows 7 SP1 and Windows 8.1 Update 1 operating systems (both 64-bit) for our test clients. These are part of a domain with a Windows Server 2012 R2 system as the domain controller.

Both the Foundation and Essentials versions of Windows Server provide simplified management options, relative to the Standard edition. This recognises that companies with 25 users or less may not have the financial resources to employ a full-time IT administrator. Consequently, some or all of the IT management tasks will be carried out on a part-time basis by staff members who may be very proficient with consumer products, but are not very familiar with business networks.

In accordance with this scenario, we have considered how easy-to-use the products would be for a non-expert administrator. We allow for the option of having an external IT consultant install and configure the software initially, and train the relevant company staff how to use it. However, in a number of cases we have noted that a high level of technical expertise is not needed to set the product up, and that non-expert administrators could perform the task themselves with help from the product manual.

Because of the emphasis on small businesses, the review covers only the essential everyday tasks needed in all networks. We have however noted that some products have additional features and could be used for significantly bigger networks. Full details of the points we have looked at for each program are given below:

Introduction and Software version reviewed

- Overview of the manufacturer's business products, and details of the product reviewed
- Main product version number of each of the components used

Supported operating systems

- Microsoft Windows operating systems supported
- Non-Windows systems supported, such as Apple and Linux (although these are not reviewed)

Additional features

- We list any features over and above what might be expected from an antivirus program, for example backup, firewall, vulnerability scanner

Documentation

- An overall view of the product's manual, and in particular whether it provides suitable instructions for installing the console and deploying client software
- Local help and online knowledge base, if available

¹ <http://www.microsoft.com/en-gb/licensing/about-licensing/windowsserver2012-r2.aspx#tab=2>

Preparing server and clients for deployment

- Any configuration of the clients and server before the endpoint protection software can be installed, e.g. opening firewall ports, enabling file sharing, or disabling User Account Control

Deploying the software²

- Installation of the console (if applicable)
- Deploying endpoint protection software to client PCs and file server, using what we regard as the easiest method for each product

Management console

- Description of layout and features

Monitoring the network

- How to see overall status of protection, including state of real-time protection and updates
- How to correct any errors in the protection status, e.g. run an update
- Reporting of malware found
- Program version installed
- Licensing information

Managing the network

- Running one-off scans
- Setting up a scheduled scan
- Running updates

Client antivirus software³

- Registration in Windows Action Center
- System Tray icon
- Is Windows Defender disabled under Windows 7, Windows 8?
- Can the user run updates and scans?
- Is there a status display which shows the local user if all is well?
- If an alert is shown that protection is disabled, how can the user re-enable it?
- What sort of alert, if any, is shown when the EICAR test file is downloaded?

Server antivirus software

- A brief overview of the server antivirus software, in the event that this is significantly different from the client endpoint protection program

² The “easiest” means of deploying a product is inevitably somewhat subjective; readers should consider whether another of the available installation methods might be better for them.

³ Some products install a minimalist user interface by default. We do not feel that this is necessarily better or worse than a fully featured client; readers should decide for themselves what best fits their own requirements.

Products reviewed

The following manufacturers participated in this review:



The manufacturers either provided us with the newest versions of their respective products, or confirmed that the latest version was available from their website (as at September 2014). The products tested for the review are listed below:

- AVIRA Endpoint Security 14.06
- Bitdefender Endpoint Security 5.3
- ESET Endpoint Security 5.0
- F-Secure PSB Workstation Security 10.10
- G DATA AntiVirus Business 13.0
- Ikarus security.manager 4.2
- Kaspersky Small Office Security 13.0
- McAfee Endpoint Security 10.0
- Sophos Endpoint Security and Control Cloud 10.3
- Symantec Endpoint Protection Small Business Edition 12.1

AV-Comparatives Approved Business Product Award 2014

We are pleased to report a very high overall standard in the products reviewed this year, all of which receive our Approved Business Product award.



As regards being user-friendly towards non-expert administrators, we feel that three of the products stand out as **especially easy to use**:

G Data Antivirus Business uses a server-based console that is particularly easy to install, well-designed, and makes deployment and managing client software simple.

Kaspersky Small Office Security has a client-integrated console that incorporates network management features into the very familiar and user-friendly window of the client software. We find this an ingeniously simple but effective solution, ideal for inexperienced administrators.

Symantec Endpoint Protection's cloud-based console displays a particularly clear and simple overview of the essentials, is extremely easy to customise, and conveniently links related pages, e.g. overall status with computer details.

Aside from ease of use, there are other factors to be considered when buying a business security product, such as system requirements, price and support. We would encourage readers to consider all the participating products, as each one has its own particular strengths. The Management Summary which follows provides an overview.

Management Summary

We have grouped the products according to the type of management console reviewed, namely self-managed, client-integrated console, cloud-based console, server-based console. Individual products are listed alphabetically within their respective group.

Self-managed

McAfee Endpoint Security Client⁴ is a very suitable standalone product for smaller businesses, which combines a familiar interface with useful business additions. These include a choice of components to be installed, a well-designed access control feature, and a concise display of recent threats.

Client-integrated console

Kaspersky Small Office Security provides an ingenious solution for businesses with up to 25 clients, with all the essential management features for a small network built into the client software. This is very easy to use, and would be particularly suitable for anyone new to network administration.

Cloud-based console

Endpoint Security by Bitdefender stands out for its excellent documentation, and the ability to customise the console. We would recommend administrators to take advantage of both of these features. A supremely easy local installation option is available, which would be ideal for non-expert admins.

F-Secure Protection Service for Business impressed us with the design of its console, which has a simple, easy-to-navigate layout, and provides a clear overview of network status on the home page. Documentation is excellent, and the client software has a familiar design.

Sophos Endpoint Security and Control Cloud includes a number of impressive features. These include the Action Center on the home page (which shows alerts and links to potential solutions), and the easy-to-use Tamper Protection, which protects client software against unauthorised access. The console is clean and easy to navigate, and client deployment very simple.

Symantec Endpoint Protection Small Business Edition is an outstanding all-round performer. The console provides excellent status reporting, and is very easy to customise to the admin's preferred content and layout. Deployment, monitoring and management of clients are all simple, while client software is clear but informative.

⁴ We have reviewed the self-managed option for McAfee Endpoint Security, i.e. the product is managed locally on each machine using the Endpoint Security Client itself. McAfee produces three different consoles that can be used to manage the Endpoint Security Client, which we were unfortunately unable to review as they were still in development at the time this review was produced. McAfee Security Center is a cloud-based solution for smaller businesses; McAfee ePolicy Orchestrator is a server-based console with maximum functionality; McAfee ePolicy Orchestrator Cloud is a cloud-based console with similar features to the server-based version.

Server-based console

Avira Endpoint Security provides a familiar, easy and intuitive experience for anyone who understands the basics of Windows administration, due to the use of standard features such as the MMC console. Documentation is excellent, client software is well-designed and familiar, and we found installing and using the product to be entirely straightforward and unproblematic.

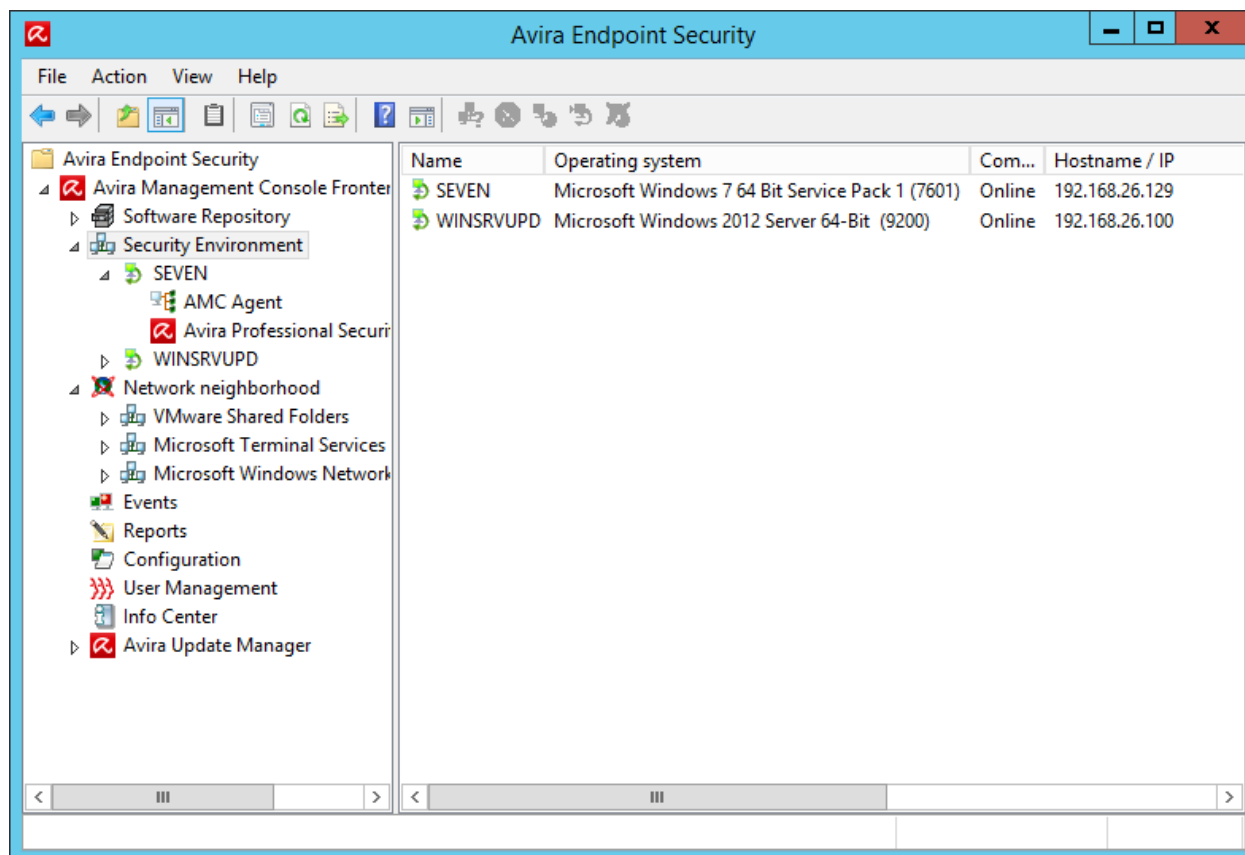
ESET Remote Administrator is a powerful console that could comfortably cope with bigger networks. Experienced administrators should find installation and deployment straightforward, especially given the outstanding help features. The interface of the client software is very user-friendly.

G Data Antivirus Business stands out for its ease of installation, deployment and management, meaning that even non-expert administrators should be able to deal with all aspects of its use. Documentation is excellent, and there is a choice of full or minimalist UI for the client software.

IKARUS security.manager provides a remarkably simple push installation process, and an ingenious means of managing individual PCs using a replica of the client software main window. The simple but clear format of the manuals make them very easy to read. Installation is entirely straightforward for an experienced administrator.

Product reviews

Avira Endpoint Security



Introduction

Avira's business range includes Professional Security (for client PCs, with management console), Endpoint Security (with additional file server protection), and Small Business Security Suite (with file and mail server protection). This review covers Endpoint Security, i.e. antivirus for client and file server systems along with the management console.

Software version reviewed

Avira Management Console 2.07.00

Avira Server Security 14.0.6

Avira Professional Security 14.0.6

Supported operating systems

According to the English version of the Avira website, Avira Professional Security runs on 32 and 64-bit Windows XP, 7, 8 and 8.1. Avira inform us that Windows Vista is not officially supported any more, but should nonetheless not have any compatibility problems.

The Avira Security Console runs on Windows Server 2008, 2008 R2, 64-bit Windows Small Business 2008 and Server 2011. Windows Server 2012/2012 R2 are not officially supported, but the console ran perfectly on our Windows Server 2012 R2 test server. Avira inform us that they are not aware of any major issues with these two variants of Windows Server.

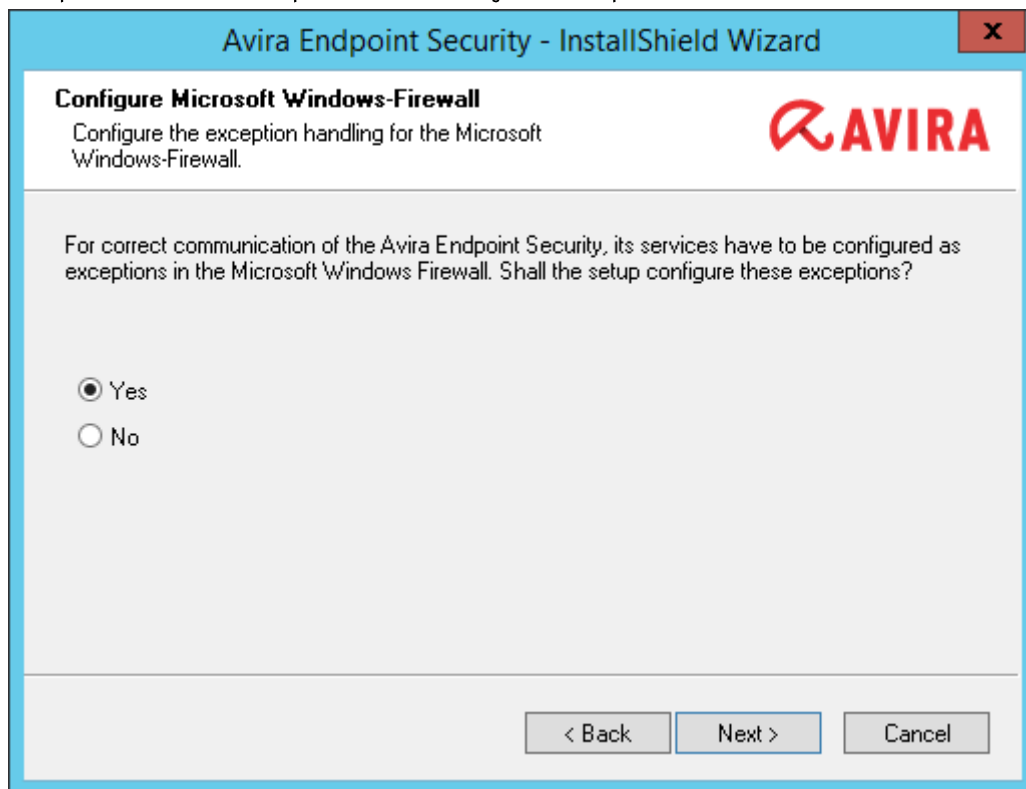
Documentation

Avira product a quick-start guide for installing the console and deploying the software, called “Avira Endpoint Security HowTo”. This is only 11 pages long, but provides all the essential instructions for the task, illustrated with screenshots. Amongst other things, it explains prerequisites of client-software deployment, such as how to enable the Computer Browser Service on the server, and Network Discovery on client computers. There are additional “HowTo” guides for the client software and file-server software, plus full manuals for all three components.

We found Avira’s documentation to be very good. The quick start guides provide essential information to get started with each product, while the full manuals are very comprehensive and detailed. All the documents are well written and produced, easily accessed through bookmarks and clickable contents pages, and illustrated with screenshots. However, we did have some difficulty finding the right manual for each product on the download page, and suggest a clearer and more consistent naming scheme.

Preparing server and clients for deployment

Preparation of both client and server systems is minimal. During the installation of the console, the setup wizard offers to open the necessary firewall ports on the server:

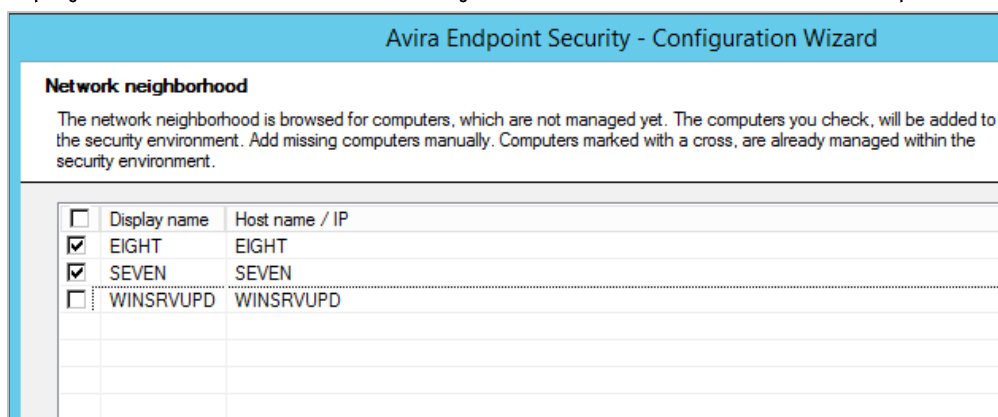


During the deployment of the client software, a message box states that the Computer Browser Service has to be enabled on the server; there are instructions in the HowTo guide for performing this operation. The only client preparation required is to enable Network Discovery (also described in the manual).

We would say that Avira makes life very easy for the administrator. Minimal preparation of server and clients required, and the necessary steps are made clear.

Deploying the software

There is a single 333 MB installer file that contains all the necessary components of the suite, i.e. the console plus antivirus software for both server and clients. This is run on the server, and the first stage involves installing the console. This requires nothing more difficult than browsing for the licence file and takes just a few minutes. As soon as the console installation has finished, the deployment wizard starts automatically. This searches the network for computers to be installed:



Client computers can be selected using the check boxes, after which the appropriate product to be installed (Avira Professional Security) is selected. The wizard then installs the software without requiring any further input from the administrator, and displays a list of the successfully installed computers at the end. The wizard can install Avira Professional Security on all Windows client computers with compatible operating systems, regardless of version or architecture, all at once. However, it needs to be run again to install Avira Server Security on the server. The procedure is identical to that for the clients.

Deploying Avira Endpoint Security is an extremely quick and convenient procedure. We would say that a non-expert administrator, guided by the manual, could carry it out without difficulty.

Management Console

Avira Endpoint Security uses the Microsoft Management Console framework. The console tree in the left-hand pane displays the main configuration and monitoring items. These are the Software Repository (software packages to be deployed to client and server computers); Security Environment (custom-made groups to which the administrator assigns computers to be managed); Network Neighbourhood (displays the computers on the network using Microsoft's Active Directory schema); Events; Reports; Configuration; User Management; Info Center (displays news items about the product, e.g. version upgrades); Avira Update Manager, which helps the administrator keep the installed software up to date. Clicking on an item in the left-hand pane displays information and configuration options; right-clicking an item in the tree displays a menu which allows the administrator to go directly to specific tasks and configuration options.

The use of the very familiar Microsoft Management Console means that IT professionals and computer enthusiasts will immediately feel at home.

Monitoring the network

Clicking on Security Environment in the left-hand pane of the window displays the status of all the managed computers. Details shown include computer name, OS, status, IP address, last notification, and products installed:

Name	Operating system	Installed products	Last notification
SEVEN	Microsoft Windows 7 64 Bit Service Pack 1 (7601)	Avira Professional Security (Windows), EN	13/09/2014 19:32:12
WINSRVUPD	Microsoft Windows 2012 Server 64-Bit (9200)	Avira Server Security (Windows), EN	13/09/2014 19:36:38

If real-time protection is disabled, the status of the computer concerned will be shown as “Product Error”, and a red exclamation mark will be displayed next to the computer’s name:

Name	Computer status	Operating system
SEVEN	Online, Product error	Microsoft Windows 7 64 Bit Service Pack 1 (7601)
WINSRVUPD	Online	Microsoft Windows 2012 Server 64-Bit (9200)

Please note that for convenience we have customised the order of columns in the above screenshots; this is easily done by drag and drop.

Expanding the computer’s icon in the left-hand pane displays two further icons, for the AMC agent and Avira Professional Security. Clicking on the latter displays a list of events for the software, including (in this case) the fact that real-time protection had been disabled. If a computer has out-of-dates signatures or a protection component is disabled, the problem can be rectified from the context menu (please see screenshot in next section).

It is possible to change the view for the Avira Professional Security item, on a per-PC basis, so that it displays the installation/activation status of individual protection components, including real-time protection.

Precise version numbers for each of the components of the client software can be found by right-clicking the Avira Professional Security icon for a particular PC, pointing to Views, and selecting Product Version.

Malware discoveries can be seen by clicking on Events in the left-hand pane, which shows all events relating to all computers on the network:

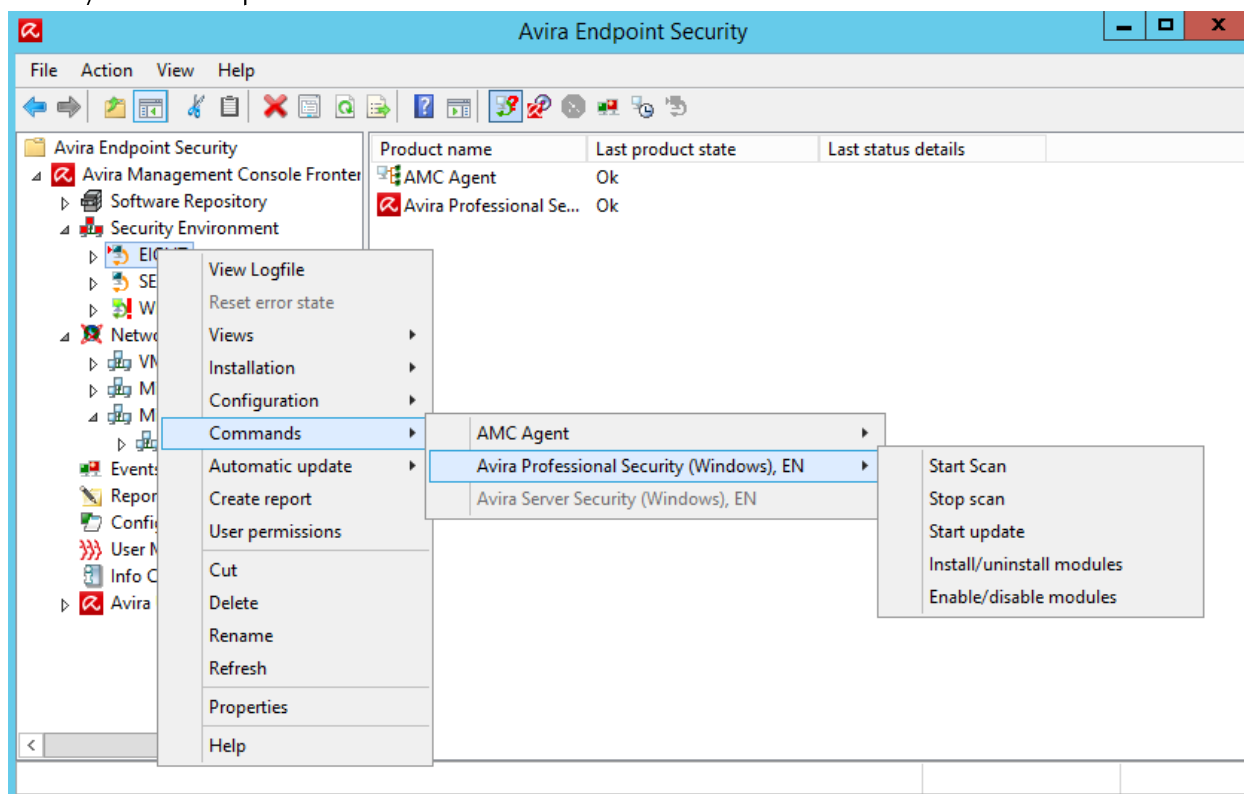
Computer na...	Level	Product	Actor	Message	Time
SEVEN	Security	Avira Professio...	Real-Time Prote...	Malware 'PFS/Amtso-Test' [riskware] was found in...	13/09/2014 19:51:57
SEVEN	Security	Avira Professio...	Real-Time Prote...	Malware 'PFS/Amtso-Test' [riskware] was found in...	13/09/2014 19:48:32
SEVEN	Security	Avira Professio...	System Scanner	Malware 'Eicar-Test-Signature' [virus] was found i...	13/09/2014 19:45:09
SEVEN	Security	Avira Professio...	Real-Time Prote...	Malware 'PFS/Amtso-Test' [riskware] was found in...	13/09/2014 19:43:52
SEVEN	Security	Avira Professio...	Real-Time Prote...	Malware 'Eicar-Test-Signature' [virus] was found i...	13/09/2014 19:42:32
SEVEN	Security	Avira Professio...	Real-Time Prote...	Malware 'Eicar-Test-Signature' [virus] was found i...	13/09/2014 19:42:30
SEVEN	Security	Avira Professio...	Real-Time Prote...	Malware 'Eicar-Test-Signature' [virus] was found i...	13/09/2014 19:42:14
SEVEN	Security	Avira Professio...	Real-Time Prote...	Malware 'Eicar-Test-Signature' [virus] was found i...	13/09/2014 19:41:59
SEVEN	Security	Avira Professio...	Real-Time Prote...	Malware 'Eicar-Test-Signature' [virus] was found i...	13/09/2014 19:41:57
WINSRVUPD	Warning	Avira Server Se...	Updater	Important new program files are available for dow...	13/09/2014 19:38:32
WINSRVUPD	Warning	Avira Server Se...	AMC Agent	The license expires in 23 day(s).	13/09/2014 19:36:58
SEVEN	Warning	Avira Professio...	AMC Agent	The license expires in 23 day(s).	13/09/2014 19:32:24
SEVEN	Warning	Avira Professio...	Real-Time Prote...	Service has been deactivated.	13/09/2014 18:08:35
SEVEN	Warning	Avira Professio...	Real-Time Prote...	Service has been deactivated.	13/09/2014 18:07:51

Alternatively, malware discoveries and other events for a particular computer can be seen by setting the view of that PC’s Avira Professional Security icon to Events. Double-clicking a malware event shows what action was taken (e.g. quarantining). We could not find any means of displaying licensing information, other than the name of the licence file.

The Security Environment view provides almost all the information an administrator could want, and as noted above, the columns can easily be dragged around as desired. We feel it would be nice if some information about malware discoveries could also be shown in the same view, although this is a minor point.

Managing the network

The Avira Management Console allows a wide variety of tasks to be carried out on a single PC or an entire group by right-clicking the group and selecting an item from the context-menu. As shown in the screenshot below, this can be used to run scans or updates, and install/uninstall or enable/disable components:

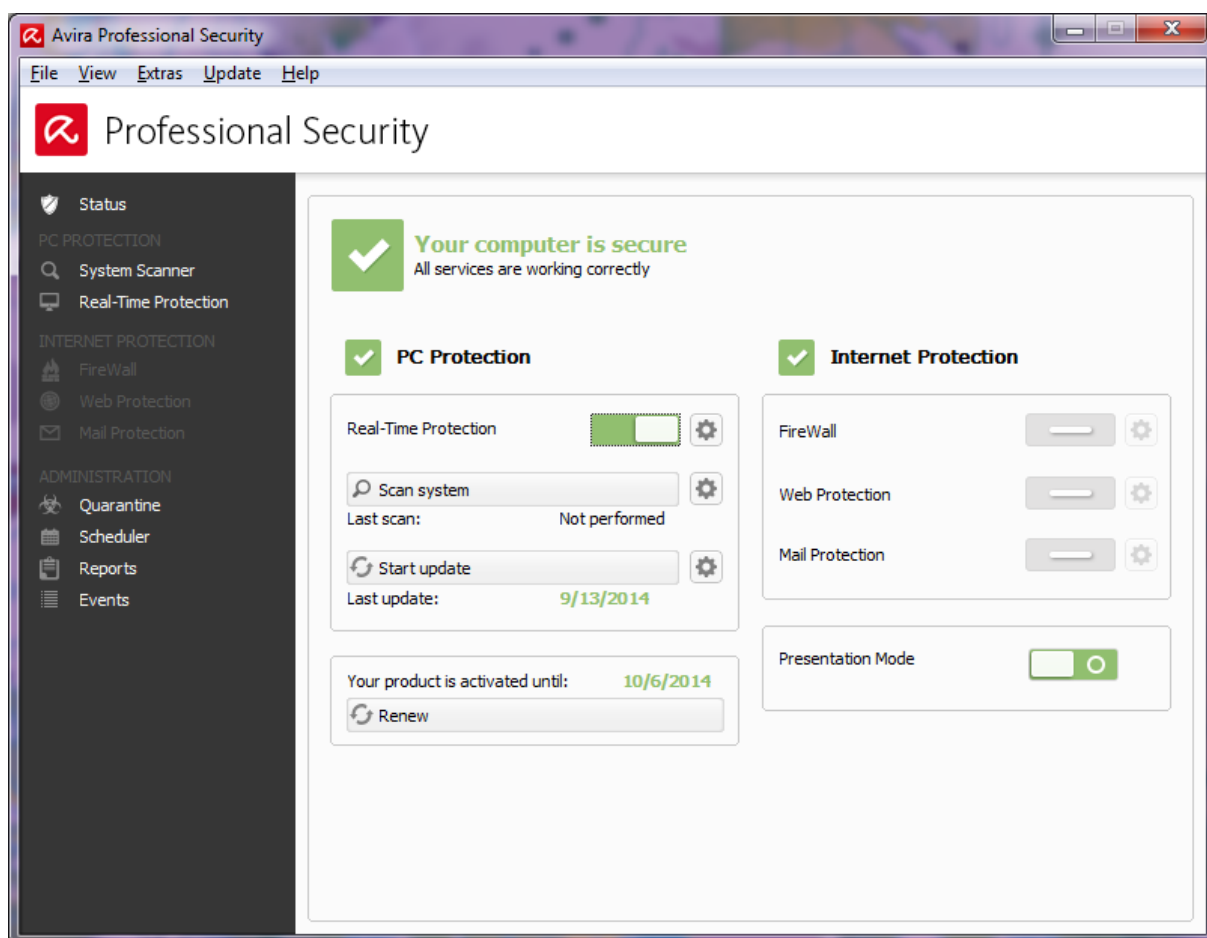


To run a scheduled scan, the administrator selects Start Scan from the context menu shown above; the dialog box that then opens allows the scan to be scheduled. Scheduling updates works in exactly the same way.

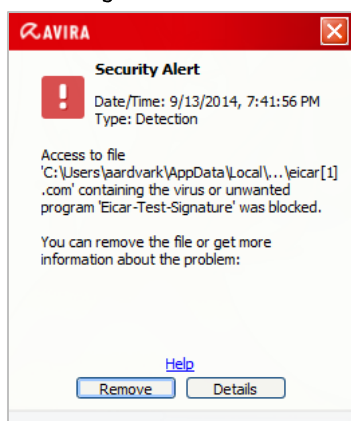
Running management tasks with the Avira console really only involves selecting the computer or computers required and right-clicking, with a wealth of commands available from the context menu. Both expert and non-expert administrators should find this very convenient.

Client antivirus software

Avira Professional Security installs a System Tray icon and registers with Windows Action Center as antivirus and antispysware. Windows Defender is disabled on both Windows 7 and Windows 8. Updates and scans can both be run directly from the status (home) page. The home page also includes a status display, with an icon and the wording "Your computer is secure" in green:



Should real-time protection be disabled, the text changes to “Your computer is not secure” with a red icon; the protection can easily be reactivated from the switch on the home page. The protection cannot be disabled from a standard user account, unless administrator credentials are entered at the Windows UAC prompt. If an attempt is made to download the EICAR test file, it is blocked and the following alert is shown:

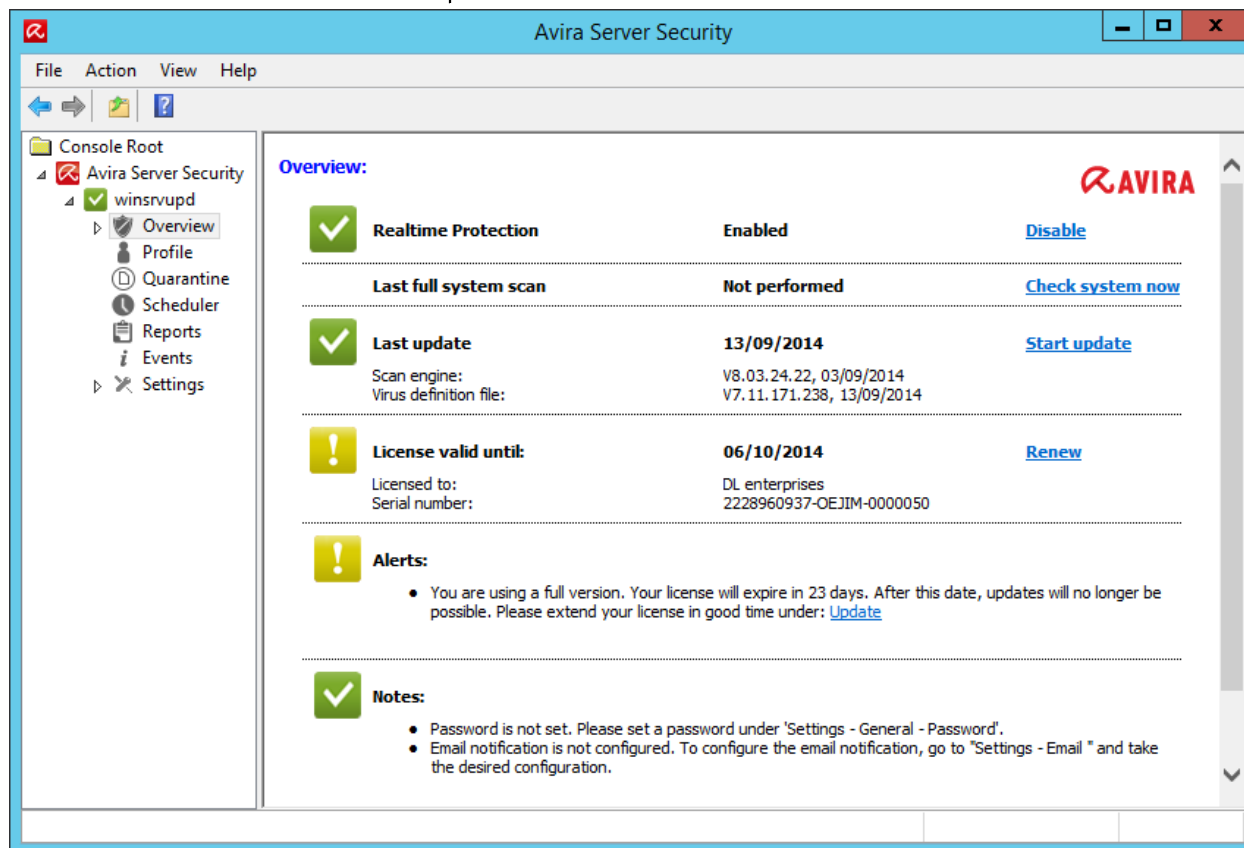


The alert persists until closed. An almost identical alert was shown for the AMTSO PUA test file too.

Avira Professional Security has an easy-to-use interface, very similar to Avira’s consumer antivirus software. It displays the status and licensing information clearly, and allows users to run scans and updates, but not disable protection, which we find ideal. We feel the malware alerts are appropriate and do not allow the user to run the malware. The software should present no problems even to non-expert administrators.

Server antivirus software

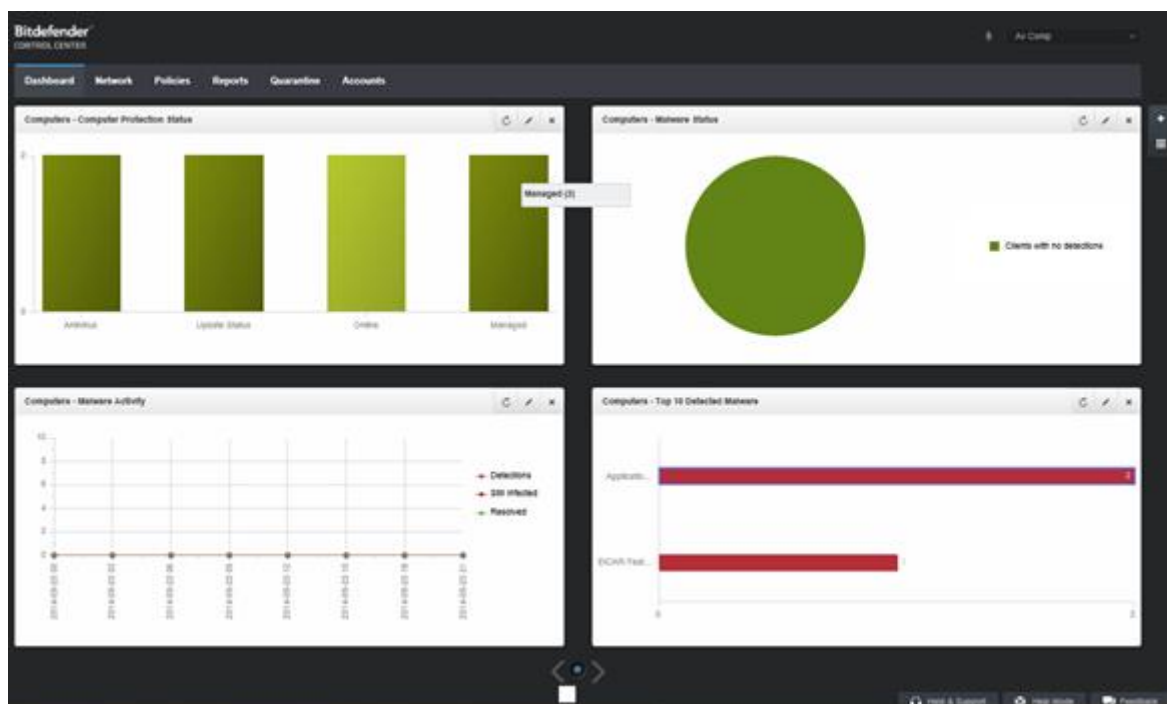
Avira Server Security displays very similar information to the client software, but in the form of an MMC console. This would allow multiple servers to be monitored from one console.



Summary

For an experienced IT professional, Avira Endpoint Security would be an entirely straightforward and trouble-free solution. We feel that with assistance from the manual, the installation and deployment processes are so simple that they should prove quite manageable for a non-expert administrator too. The console may require just a little exploration before everything becomes clear, but the familiar MMC console and sensible layout ensure that important functions and information can be found quite easily. The documentation is very well produced and comprehensive.

Bitdefender Small Office Security (cloud)



Introduction

Bitdefender make a variety of business security products, for companies of all sizes. GravityZone is an on-premise console that can manage Windows desktops and servers, Mac and Linux clients (all including virtualised and hardware), Android and iOS devices. Here we have reviewed Small Office Security, a cloud-based console based on Gravity Zone architecture that can manage Windows desktops and servers, and Mac clients.

Software version reviewed

Small Office Security Control Center as at 23rd September 2014
Endpoint Security by Bitdefender 5.3.13

Supported operating systems

Clients: Windows 8, 8.1, Windows 7, Windows Vista (SP1), Windows XP (SP3)
Server: Windows Server 2012, 2012 R2, 2008, 2008 R2, 2003 with Service Pack 1 and 2003 R2;
Windows Small Business Server 2011, 2008 and 2003; Windows Home Server
Embedded: Windows Embedded 8.1 Industry, 8 Standard, 7 Standard, 7 Compact, 7 POSReady 2009, Standard 2009.
Non-Windows OS: Mac OS X Lion 10.7, 10.8, 10.9

Additional features

Intrusion detection system, web access control, anti-phishing, category control, data protection, application control

Documentation

There are two manuals for the product, a 38-page Quick-Start Guide, and a 155-page Administrator's Guide. The Quick-Start Guide, as the name suggests, covers the basics of connecting to the console, deploying the client software, and the most essential tasks such as monitoring the network and

scanning client PCs. The Administrator's Guide also covers these points, along with comprehensive instructions for all aspects of managing the system. Both documents are bookmarked, have clickable contents pages, and are illustrated with screenshots. There is also an online knowledge base, with articles for relevant, frequently asked questions such as "How to prepare workstations for Endpoint Security automatic deployment". Each article provides step-by-step instructions, abundantly illustrated with screenshots.

We regard Bitdefender's documentation as outstanding. Firstly, the two manuals can easily be found by clicking the "Help and Support" link on the main page of the console. They are both produced to the highest possible standards, clearly written and laid out, and illustrated with screenshots wherever appropriate. The bookmarks and clickable contents pages make navigating the documents easy. The Quick-Start Guide provides just the right amount of information to get the system up and running. The Knowledge Base articles are of an equally high standard.

Preparing server and clients for deployment

The first computer on the network has to be installed locally. This does not involve any additional configuration. The remaining computers can be installed locally or remotely. If the latter method is used, the administrator has to check that the admin\$ file share is enabled, switch off simple file sharing, and temporarily disable both UAC and the Windows Firewall. This is very clearly described in the Quick Start Guide under Remote Installation Requirements.

Deploying the software

The console is cloud-based and so no installation is required; the admin just enters the URL in a browser and logs in. The antivirus software can be deployed to client PCs and the server by local installation or push installation. Local installation effectively involves downloading an installation package from the console and running it on the local machine.

To enable push installation, the first computer to be installed (the server is ideal, as it is always on) has to be designated as an Endpoint Security Relay during installation. Target PCs have to be prepared as described above, and then the endpoint security software can be pushed out to the clients from the console.

We used the local installation method in our test, and suggest that it would be ideal for non-expert administrators, as it is really no more difficult than installing iTunes.

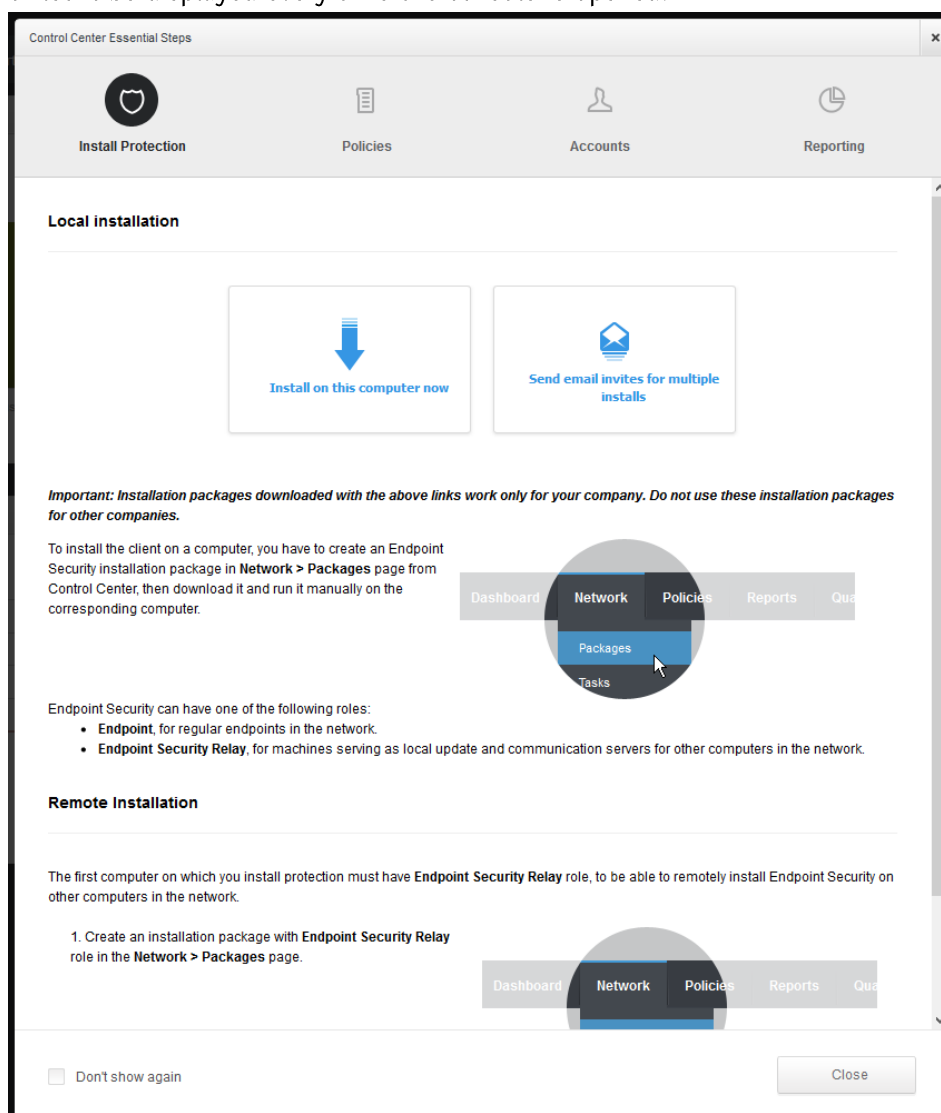
Management Console

The Dashboard (home page of the console) shows four large boxes with status information: Computer Protection Status, Malware Status, Malware Activity, and Top 10 Detected Malware. The Dashboard is very customisable; the administrator can move the status boxes around, create additional pages for additional items, or delete existing items and replace them with others. The list of items that can be displayed is shown below:



Every box has Close, Edit and Refresh buttons. There is a menu bar along the top of the page, from which different pages can be displayed: Dashboard, Network, Policies, Reports, Quarantine. In the bottom right-hand corner are three help-related menus.

When the admin first logs in to the console, the Control Center Essential Steps page is shown, which provides installation instructions and links. The admin can select “Don’t show again” to suppress it, or let it be displayed every time the console is opened.



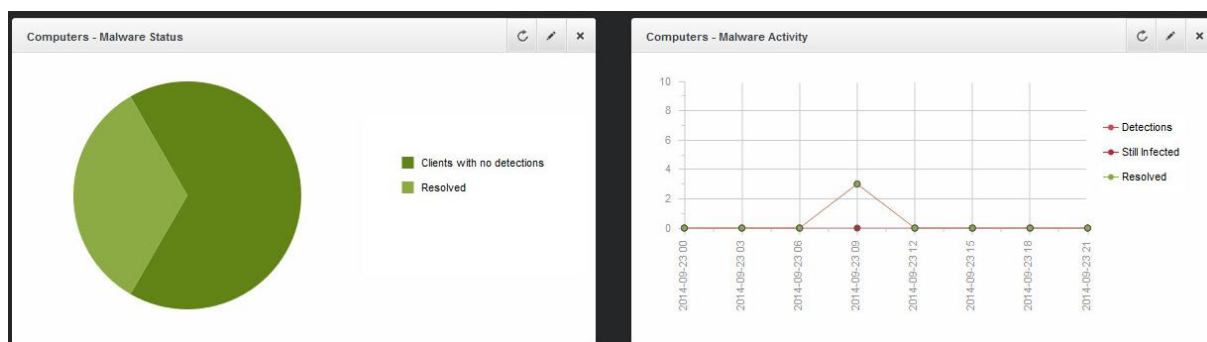
We feel that the console is clean and uncluttered, and does not overwhelm the admin. We would prefer to see some different items (such as Update Status) on the home page, but the customisation feature lets admins do precisely that. The option to show the installation page when the admin logs in strikes us as very useful.

Monitoring the network

The default dashboard view displays the Computer Protection Status, which shows the admin if all protection components are enabled on all clients. There is also a Network Protection Status element (which indicates the update status), but this is not displayed by default and has to be added to the console manually.

For both the Computer Protection Status and the Network Protection Status, clicking on the relevant graph opens a page with more specific information, showing exactly which clients are affected by which problem. However, we could not find any means of rectifying any of the problems on either page; to run an update or reactivate real-time protection, the admin has to manually create a task or reassign a policy.

Three of the four default elements in the dashboard relate to malware discoveries. Current status and dates of detections are illustrated below:

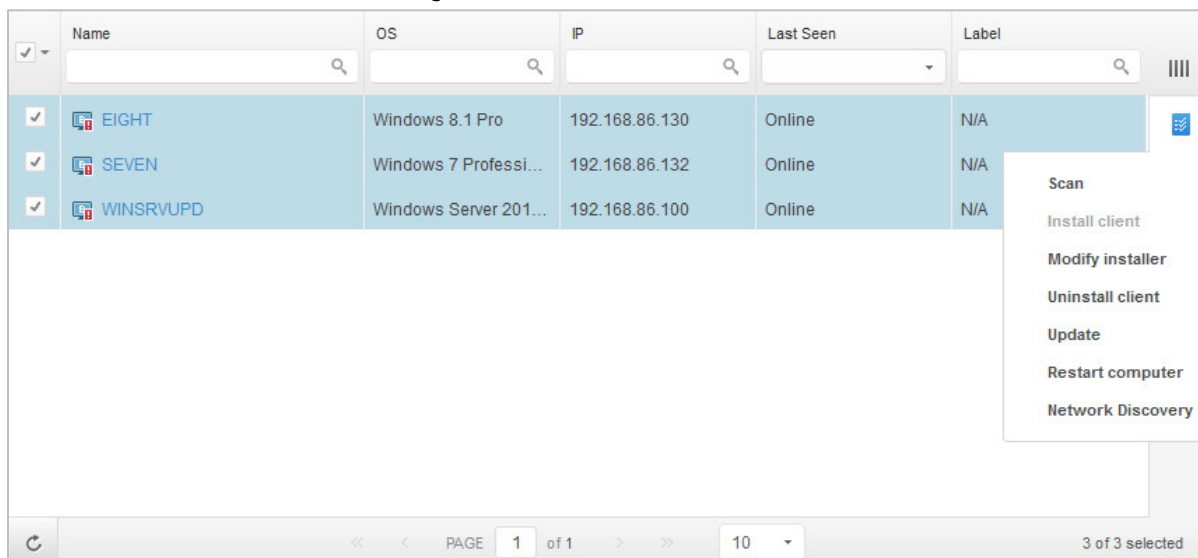


The program version running on individual client PCs can be seen by opening the Network page to display all managed computers, and clicking on an individual computer to display its properties. Licensing information can be viewed by clicking the “My company” entry in the menu in the top right-hand corner of the console.

We feel that default dashboard display, whilst very clear, puts too much emphasis on malware finds; Network Protection Status, which warns if signature are out of date, could in our opinion replace one of the malware-found items (admins can do this themselves as the console is customisable). We also think it is a shame that there is no link between the warnings shown in the console and the means of putting the problem right. We suggest it would be a significant improvement if the admin could click on a graph showing clients with outdated signatures, and be taken to a page where an update could be carried out. We do however note that the action currently required is well explained in the manual.

Managing the network

Scans and updates can be run from the Network page by selecting the computer(s) required, clicking the Tasks button, and then selecting the task to be run:

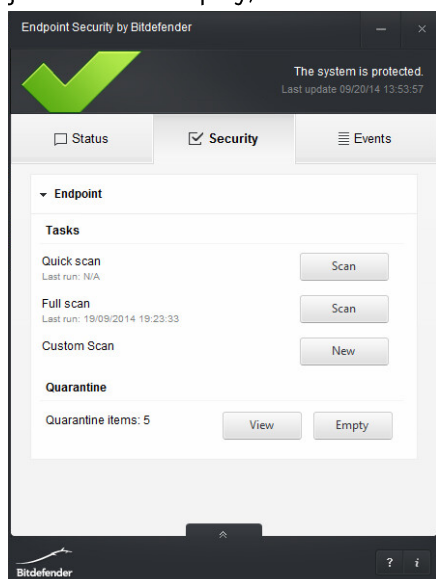


Scheduling scans can be configured using Policies. This involves creating a new policy, and configuring the scan settings to run on the desired schedule. Updates can be scheduled in the same way.

Running scans and updates from the Network page is very straightforward. Using Policies to schedule the items was not quite so intuitive in our view, and we wonder whether it might not be possible to provide a link within the tasks to the scheduling function in Policies. We were also slightly confused by the Tasks page, which shows tasks already created but does not allow new ones to be made (this has to be done from the Network page).

Client antivirus software

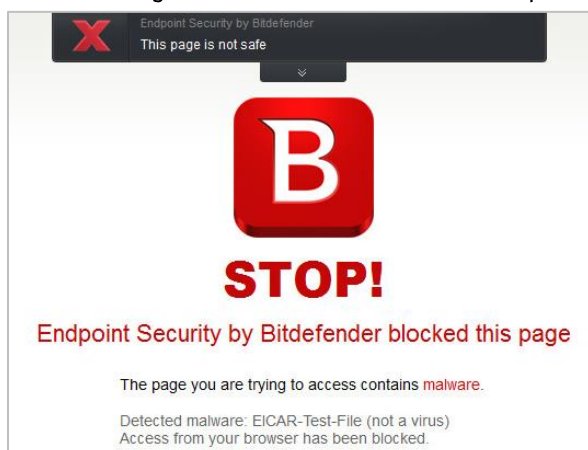
Endpoint Security by Bitdefender installs a System Tray icon. It registers with Windows Action Center as antivirus, antispysware and firewall. Windows Firewall and Windows Defender are disabled in both Windows 7 and Windows 8. When first opened, the software has a minimalist interface with just a status display, but this can be opened out to show scanning tasks and access to quarantine:



The update function can be started by right-clicking the system tray icon and clicking about; progress can be seen in the About box. We do not feel this is an obvious way of running an update, although updates are run automatically on a schedule. If a protection component is disabled a warning is shown. However, there is no means of reactivating it or contacting the administrator from the client software; users who see the warning can only send an email or shout across the office.

It is not possible to disable protection components from the client window, regardless of which user account is used; it can only be done from the console. This prevents users from switching the antivirus or firewall off without authorisation.

The following alert is shown when an attempt is made to download the EICAR test file:



Some administrators will favour the fairly minimalist interface of Endpoint Security for Bitdefender. It certainly prevents users from disabling anything that they shouldn't, and does not require any sort of action to be taken when malware is found. We do however feel that there should be some means of reactivating protection when a warning to this effect is displayed, or at least a quick and easy means of contacting the administrator.

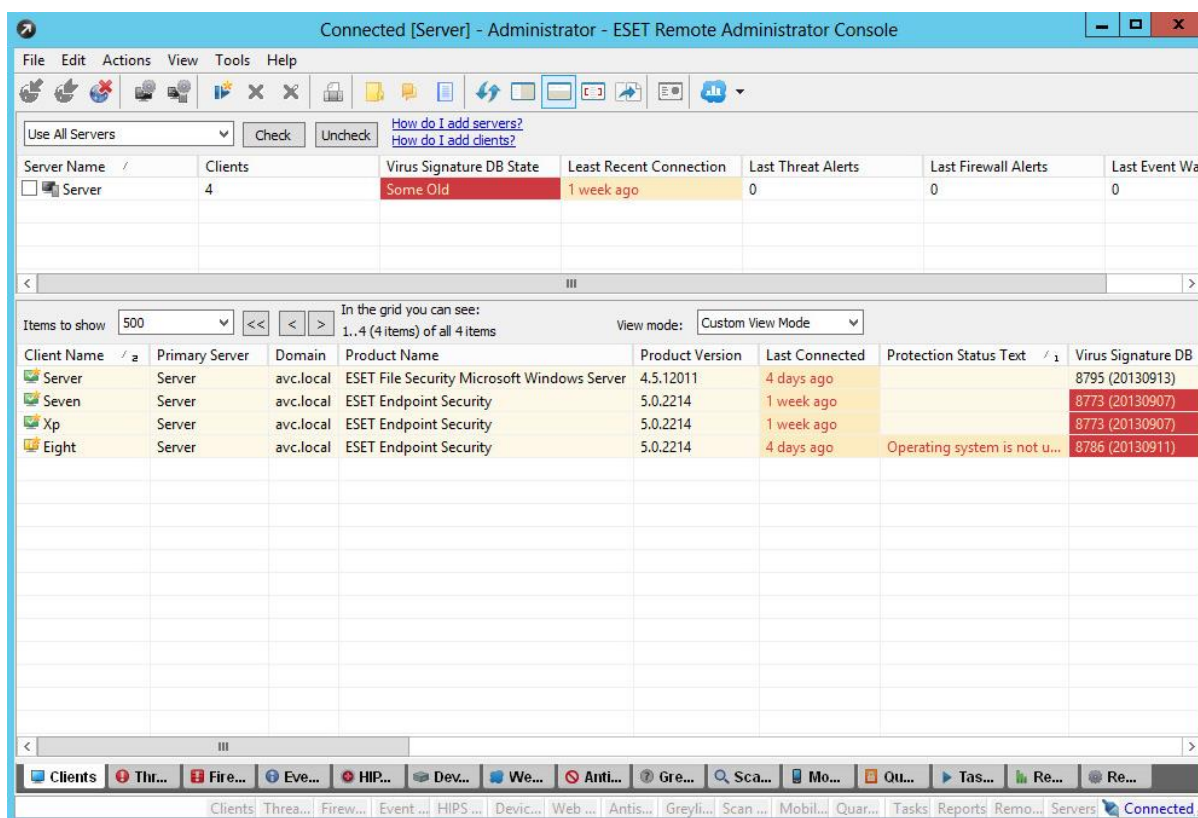
Server antivirus software

The protection software installed on the server is identical to that used for clients, except that the Content Control and Firewall components are not installed (Windows Firewall is not disabled on the server).

Summary

Deployment of Endpoint Security by Bitdefender could easily be managed by a non-expert administrator in a small business. The web-based GravityZone console requires no installation, and the client software can easily be deployed on clients by installing it locally on each client; this is made especially easy by the Control Center Essential Steps page, which is shown when the admin logs on to the console. The console Dashboard displays the status of the network in the form of big, clear, coloured graphics, making it very easy to get an overview of the situation at a glance. We would however suggest that admins might like to take advantage of the customisation feature to change some of the items shown on the first page of the Dashboard. In some areas, we found management not quite as intuitive as we would like, and suggest links from one element to another might be helpful. However, the outstanding documentation easily compensates for any slight confusion in the interface, with instructions for all essential tasks easily accessible, clearly explained and very well illustrated. We would suggest that even non-expert administrators will cope well with managing the product provided they read the manual first.

ESET Endpoint Security



Introduction

ESET's business security range includes client antivirus and endpoint protection, mobile security, file and mail server protection, gateway and collaboration security. This individual product review covers the current versions of ESET Endpoint Security client software, ESET File Security for Windows Server, and the Remote Administrator console.

Software version reviewed

ESET Remote Administrator Server 5.2
 ESET Remote Administrator Console 5.2
 ESET File Security 4.5
 ESET Endpoint Security 5.0

Supported operating systems

ESET Endpoint Security runs on 32 and 64-bit versions of Windows XP, Vista, 7 and 8. ESET File Security runs on Windows 2000 Server, 32 and 64-bit versions of Windows Server 2000, 2003 and 2008, 64-bit Windows Server 2008 R2, 2012 and 2012 R2, including Small Business Server variants. The ESET Remote Administrator Server and Console run on all of the client and server versions of Windows listed above.

ESET's protection for Mac OS X, Symbian, Windows Mobile, Exchange, SharePoint Protection and Android can be managed from the console.

Additional features

Client firewall, Web Control, Device Control, ESET SysInspector, ESET SysRescue.

Documentation

ESET produce two manuals for Remote Administrator, a very comprehensive 122-page User Guide, and a succinct 13-page Quick Start Guide. Both are illustrated with screenshots, and accessible via clickable contents pages and bookmarks. The Quick Start Guide states the estimated time needed for each particular configuration job, and integrates its instructions with the screenshots, using a translucent blue overlay to connect the text on the left with the screenshot on the right:

Section 3: Setting up the Mirror server

Your ESET-protected client workstations get regular updates to the virus signature database from ESET servers. This keeps them current and protected from evolving threats. Having all your clients connect to the ESET servers independently would result in an unnecessary amount of traffic across your local area network (LAN).

ESET Remote Administrator provides a Mirror server (a server that "mirrors" the content available on ESET servers) on your own LAN. This way your clients only need to check locally for new virus signature updates and program component updates.

3.1 Mirror server setup

Open the ESET Remote Administrator Console by clicking **Start → All Programs → ESET → ESET Remote Administrator Console → ESET Remote Administrator Console**. Verify that you are connected to the ESET Remote Administrator Server (**File → Connect**).

In this guide, we're going to use the default Mirror server configuration using internal HTTP. There are other options available, including using a local folder to store update content, as well as instructions for creating replicated Mirror servers for different LANs. See the KB connection at the right for more information.

Click **Tools → Server Options**. Click the **Updates** tab and enter your ESET-issued Username and Password in the **Update Username** and **Update Password** fields in the **Server Options** window (Figure 1-1, at right). Click **Set Password...** to enter your Password.

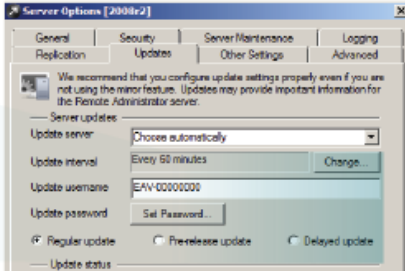
Estimated time: 15 minutes

KB connection

Check the ESET Knowledgebase for more info:

How do I install ESET Remote Administrator and configure a Mirror server? (5.x)

<http://kb.eset.com/ezetkb/SOLN2993>



Also visible in the screenshot above is a link to the appropriate page of the online Knowledge Base; this provides additional articles, and includes not only annotated screenshots but also instructional videos.

ESET's manuals and knowledge base are first class, in our opinion. The Quick Start Guide is ideal for setting the software up, and we found the KB links, time estimates and connection between text and screenshot very helpful.

Preparing server and clients for deployment

In order to enable communication between clients and the administration server, a number of ports have to be opened in the server firewall. The Quick Start Guide notes this, and directs the reader to the appropriate section of the User Guide, where complete details are provided.

If push installation is to be used to deploy the software to the clients, several items have to be configured on the client PCs. These vary somewhat depending on Windows version, but include removing any existing antivirus software, opening firewall ports, disabling User Account Control, and enabling the Remote Registry Service. The Quick Start Guide provides full details.

Familiarity with configuring a number of Windows components is required for the preparation of the server and clients, especially if push installation is to be used. Consequently, we suggest that it is a task best carried out by a professional administrator.

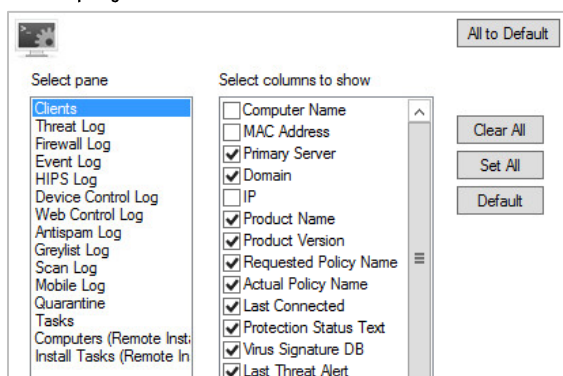
Deploying the software

4 or 5 files have to be downloaded: 2 console components, 32 and/or 64-bit client installers, and the file-server installer. ESET's management system involves a console called Remote Administrator, which runs on the local network. It has two components, Server and Console. The Server component provides the functionality, and runs on one machine in the network; the Console provides the user interface, and can be installed on multiple computers. Deployment of the client software by push installation involves creating 32 and/or 64-bit client installation packages from the .MSI installer files, running a network search for client machine(s) to be installed, and selecting those to be installed. As an alternative to push installation, the administrator can create an installation package for local installation, which is then run on individual client PCs. The file-server antivirus software can be installed locally or by separate push installation.

We recommend reading the Quick Start Guide in its entirety, and following up appropriate references to the User Guide or online Knowledge Base, before starting the deployment. Having done this, an experienced administrator should find installing the console and deploying the client software to be very straightforward. We would definitely advise small businesses without dedicated IT staff to have the system set up by an IT professional, however.

Management console

The layout of the ESET Remote Administrator console is fairly similar to Microsoft's MMC consoles. There is a menu bar and toolbar along the top, with a narrow left-hand pane and larger right-hand pane. Additionally, a row of tabs along the bottom of the window allows a wide variety of views to be shown in the main pane, including Clients, Threats, Quarantine, Tasks, Reports, Remote Install, and various logs. We note that the content of all the pages of the console can be customised extensively. The order of the columns can be changed easily by drag and drop, and the columns to be displayed can be added or removed:



We found that the array of available tabs, buttons, menus and links in the console did not make it easy to obtain an overview. For experienced admins, a little practice would be sufficient to find their way around. However, we would suggest that non-expert administrators might like to have a professional IT consultant talk them through the most important functions of the console, and perhaps make use of the customisation feature to filter out non-essential items. We note that a very well-designed web-based console, which displays a very clear overview, is included in the package.

Monitoring the network

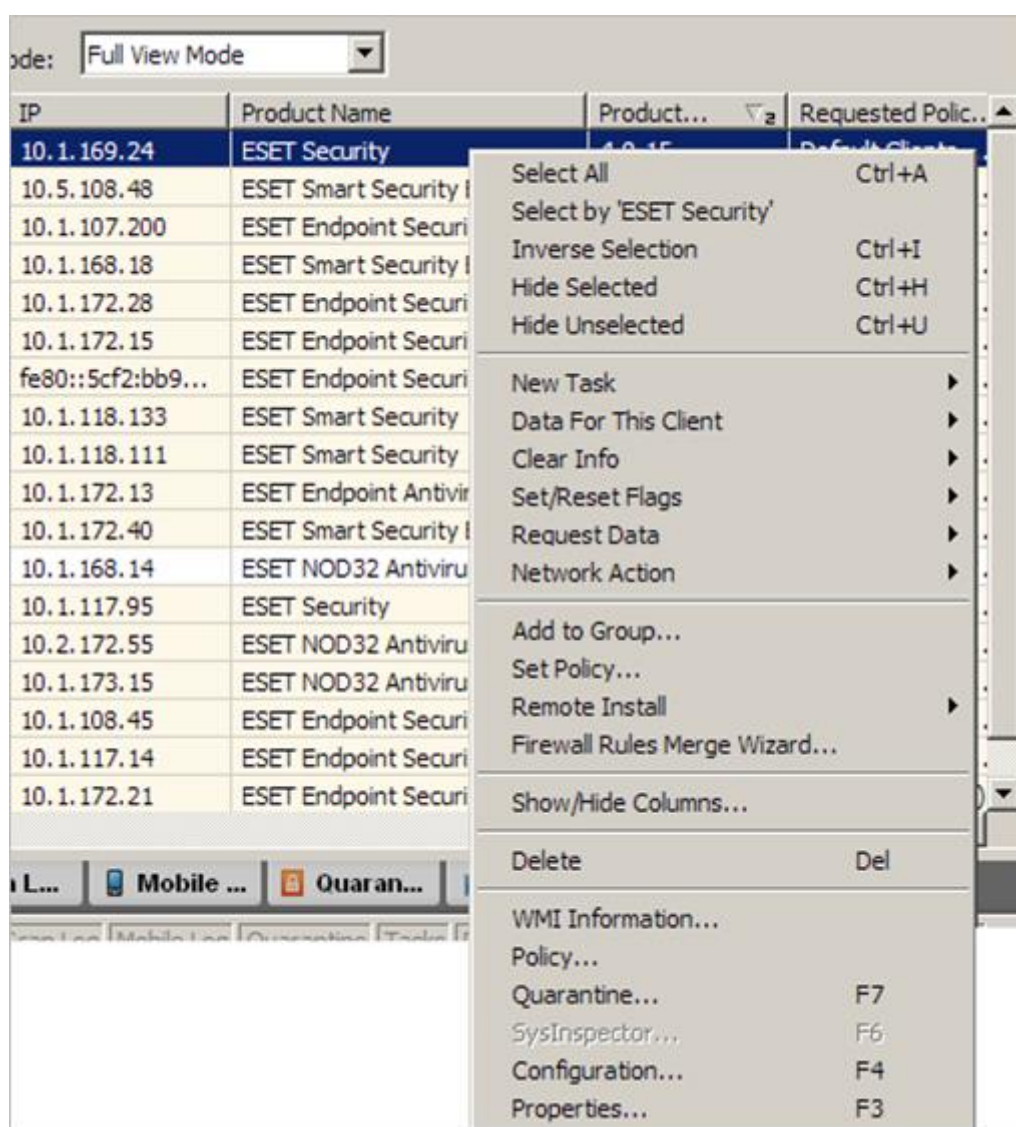
The Clients page of the ESET Remote Administrator console displays information about each of the monitored computers, including protection status, virus signature database version and date, product name and version number of the software installed, and last malware discovery. The Protection Status Text column displays the same information that is shown in the ESET window on

the client; this indicates whether essential components such as real-time protection and firewall are active, signatures are up to date, and whether important Windows Updates are available for the client operating system. Licensing information can be found in the License Manager (Tools menu). This shows the current licence, the number of client licences in total, how many of these are free, and the licence expiry date. Malware discoveries are shown on the Threat Log tab.

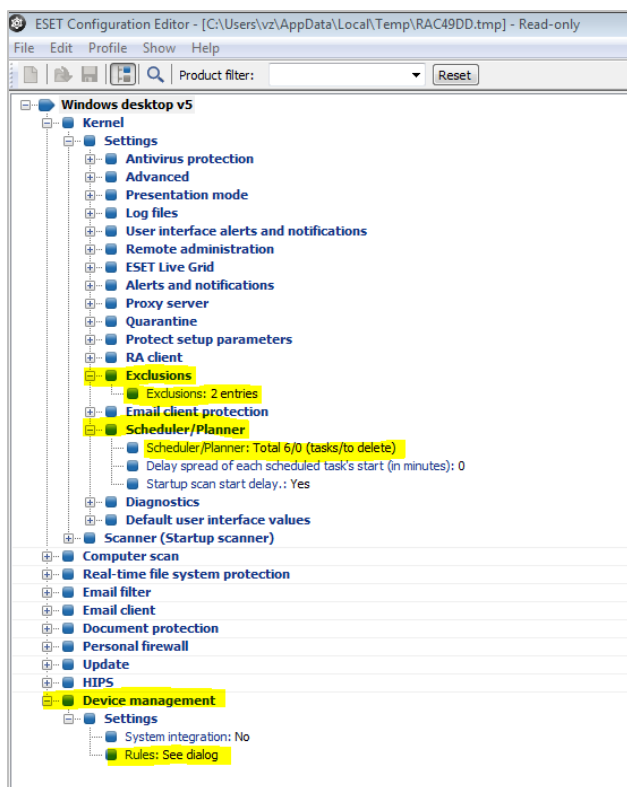
We feel the Clients page of ESET Remote Administrator displays the most important status items at a glance. We like the customisation feature, which could be used to add or remove columns or change their order, to the individual administrator's taste.

Managing the network

Right-clicking one or more selected computers in the Clients tab allows a number of different tasks to be started from the New Task sub-menu. These include full or custom scans, updates, and activating or deactivating specific components such as real-time protection.

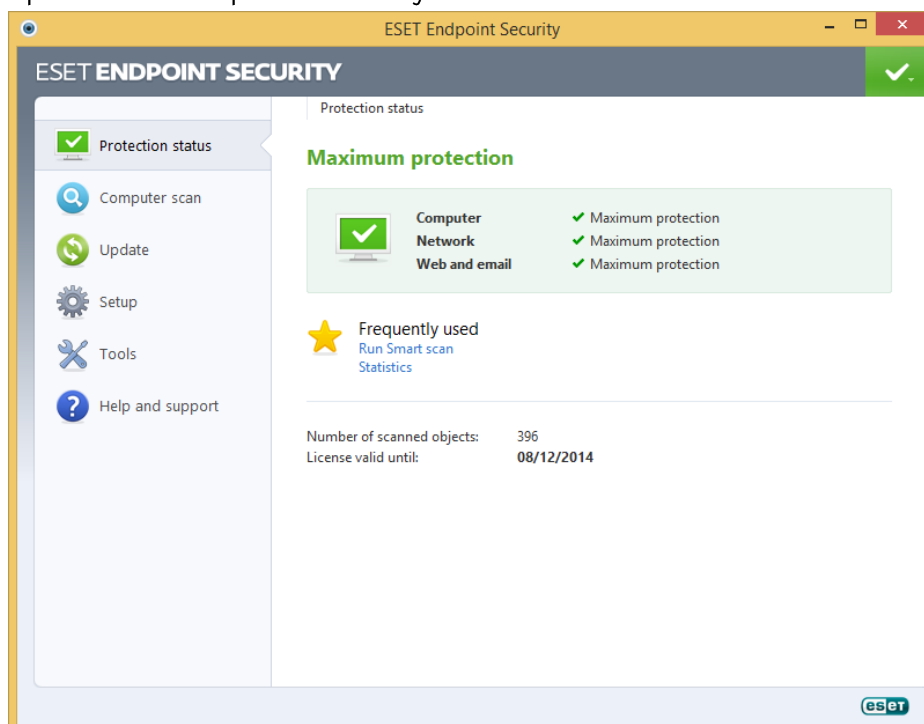


Scheduling scan and signature updates, adding scanning exclusions, and device control are all performed using the Configuration Editor:

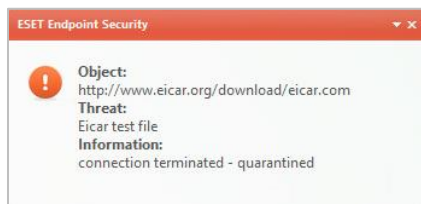


Client antivirus software

ESET Endpoint Security installs a System Tray icon, and registers with Windows Action Center as antivirus, antispyware and firewall. Windows Firewall is deactivated, as is Windows Defender in Windows 8 (but not the antispyware-only version in Windows 7). There is a very obvious status display in the form of a green text heading plus tick (checkmark) symbol when all is well; in the event of a problem, the text turns red and becomes a warning message, while the symbol changes to an exclamation mark. A text link is provided which will reactivate the protection when clicked. Update and scan options are easily accessible from the menu bar on the left-hand side.

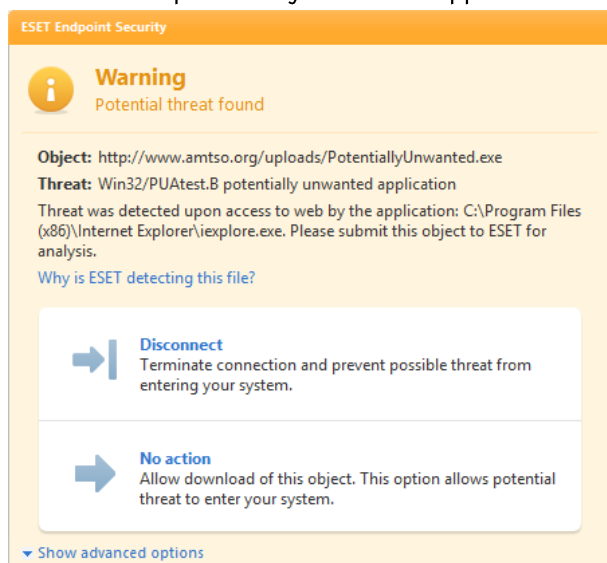


When using a standard user account, it is only possible to disable protection components such as real-time protection if administrator credentials are entered at the UAC prompt. When the EICAR test file is downloaded, ESET blocks the download and displayed this warning message:



We feel this makes reasonably clear to the user that no further action is required.

If the AMTISO potentially unwanted application is downloaded, the user is given a choice:



Some administrators might not want their users to run potentially unwanted applications; however, if "Display Alerts" is deactivated in Advanced Setup\User Interface, the file is blocked and a notification is displayed that does not allow the user to run the software.

Server antivirus software

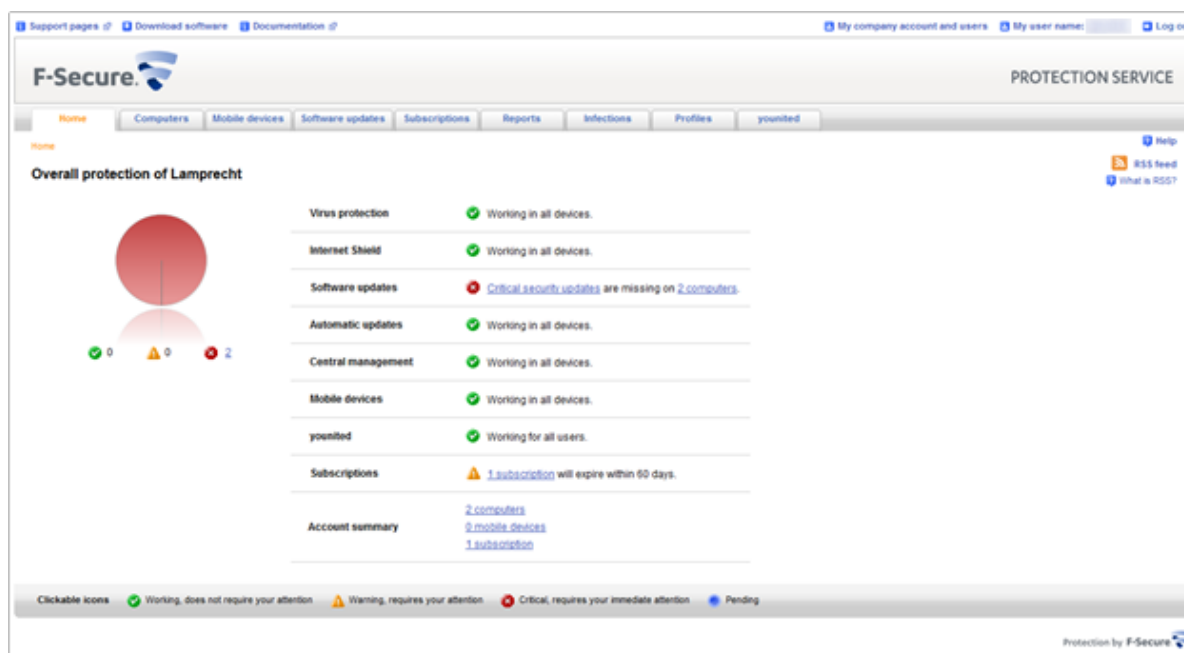
In terms of the user interface, the file server antivirus software can be regarded as identical to the client endpoint protection.

The interface of ESET's antivirus/endpoint-protection software is exemplary, in our opinion. All important functions and information are easy to find in a very clean and uncluttered window. Standard users can run updates and scans, but not disable protection; we regard this as optimal.

Summary

ESET's Remote Administrator as a very powerful console with the capability to handle larger networks as well as small businesses. For experienced administrators, deploying and using the software should be very straightforward, given the outstanding quality of the manuals and knowledge base. However, we recommend small businesses without dedicated IT staff to have an IT professional install and configure the software, and train the staff members who will carry out the everyday management. The antivirus software for the server and clients is a model of simplicity and clarity.

F-Secure Protection Service for Business



Introduction

F-Secure produce a wide range of products for businesses large and small, including endpoint security for Windows, Mac OS X, Linux, and various mobile platforms, plus protection for file servers, mail servers and gateways. We have reviewed F-Secure Protection Service for Business, which is aimed at small businesses, and uses a web-based console to monitor antivirus software for clients and file servers.

Software version reviewed

PSB Workstation Security 10.10

PSB Console as at 30th September 2014

Supported operating systems

Microsoft® Windows:

Windows 8 & 8.1, Windows 7, Vista (32/64-bit), XP

Windows Server 2003/R2, 2008/R2, 2012, 2012 Essentials

Small Business Server 2003/R2, 2008, 2011, 2011 Essentials

Non-Windows platforms:

CentOS 5.5, 6.4, 6.5

Debian 6.0, 7.0

Red Hat Enterprise Linux 5.5, 5.9, 5.10, 6.4, 6.5

SUSE Linux Enterprise Server 11 SP1, SP3

Ubuntu 10.04, 12.04 and 12.04.2

Mac OS X 10.6, 10.6.8, 10.7, 10.8

Android 2.2, 2.3, 3.0, 3.1, 3.2, 4.0, 4.1, 4.2, 4.3

S60 3rd, 5th edition, Symbian 3

Windows Mobile 5/6.x

Blackberry 5, 6, 7 (Antitheft)

Additional features

Client Firewall, software vulnerability scanner & updater, safe file storage, sync & share.

Documentation

F-Secure provide two manuals for the product, a 24-page Getting Started Guide, and a 54-page Admin Guide. The Getting Started Guide covers the basics of setting up the system, starting with creating an account, and finishing with deployment instructions for workstations, servers and mobile devices. The Admin Guide also covers these, and includes additional instructions for monitoring and managing the software. Both manuals are produced to a high standard, clearly laid out and accessible via bookmarks and clickable contents page, and illustrated with screenshots. There is also a knowledge base on F-Secure's website, which provides answers to 20 common questions.

We would describe the documentation for F-Secure PSB as very good.

Preparing server and clients for deployment

We did not need to make any preparation of either the client or the server before deploying the endpoint protection software.

Deploying the software

The console is cloud-based and so requires no installation; the admin simply goes to the URL and logs in. The endpoint protection software can be installed by downloading the setup file from the console and running it locally on each computer. Alternatively, the console allows the admin to enter users' email addresses and email a link from which users can install the software themselves; a remote push installation is also possible. The local setup process requires very little intervention. There is a choice of languages and the installation folder, and the licence key has to be entered.

We found the local installation process to be no more complicated than installing iTunes. It could easily be performed by a non-expert administrator, especially as both manuals provide very clear illustrated instructions. We feel this makes it ideal for small businesses without their own IT staff.

Management Console

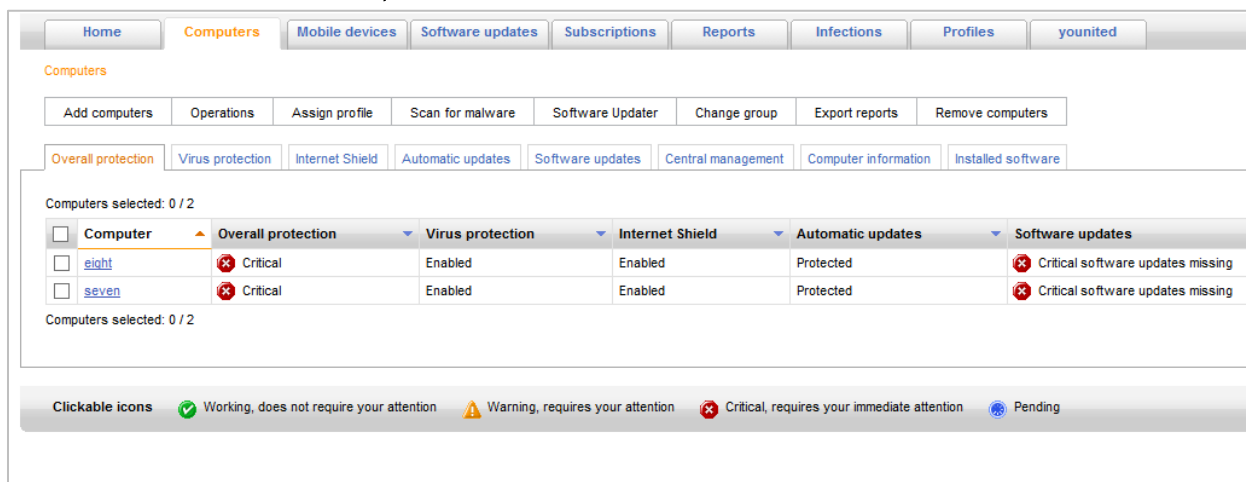
The web-based console has a single-pane design. Different pages can be shown by clicking on a row of tabs along the top, which include Home, Computers, Mobile Devices, Software Updates, Subscriptions, Reports and Infections. Home shows the overall status of the network, while Computers shows a list of individual computers with their own specific status. The Software Updates tab informs the admin of missing updates for Microsoft and other third-party vendors, not just F-Secure itself. There is a menu bar at the top, with links related to help, F-Secure account, and software downloads.

We feel the design of the console is particularly clear and easy to understand. Navigating involves one single line of tabs at the top, and individual pages are kept clean and simple, enabling the admin to find the relevant information or function very quickly. This would make it particularly suitable for non-expert administrators, although IT professionals will doubtless appreciate the console's clarity too.

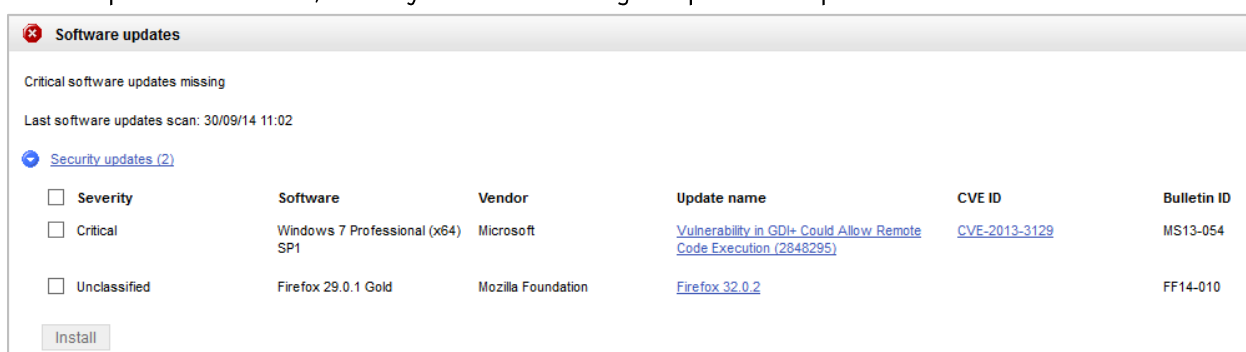
Monitoring the network

The overall status of devices on the network is shown on the home page (please see main screenshot above). This shows a list of components within the endpoint protection software; if there are no problems on any devices, the status is shown as "Working in all devices". If there is a problem, the

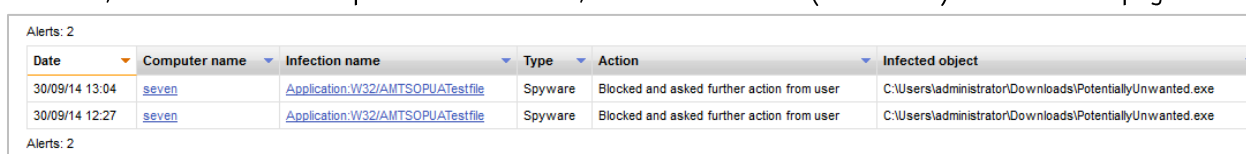
status display shows what it is and how many computers are affected, e.g. “Critical security updates are missing on 2 Computers”. The alert text is a link to the Computers tab, which allows the administrator to see which computers are affected:



Clicking on an individual computer’s name opens its information page, which provides a detailed status report. In this case, an easy means of solving the problem is provided:



Malware detections are shown under the Infections tab. If they have been dealt with by the client software, and thus do not require further action, no alert is shown (or needed) on the Home page.

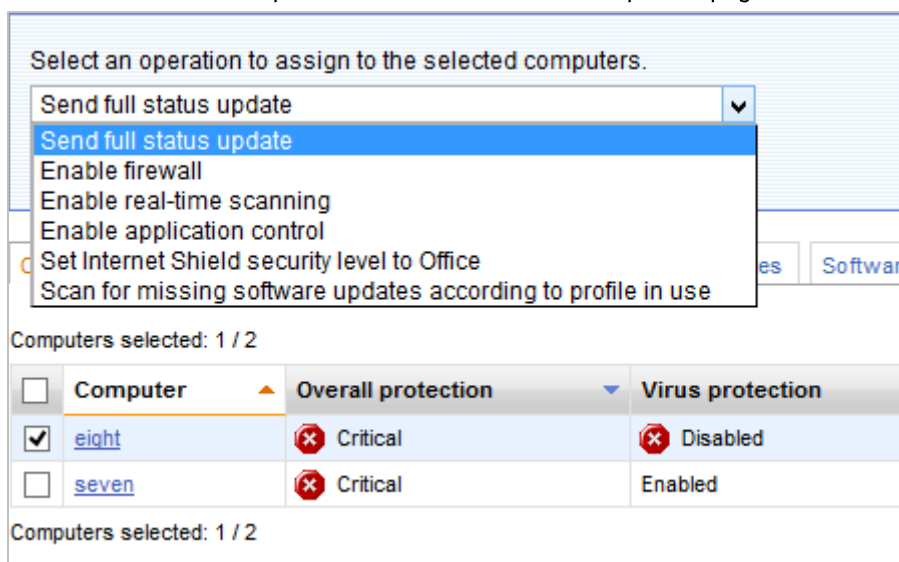


The sub-tabs of the Computers tab allow the admin to see various items, including the status of real-time protection (Virus Protection), Firewall (Internet Shield), malware signatures (Software Updates), F-Secure client software version and licence key (Installed Software), plus operating system and IP address (Computer Information).

We feel F-Secure PSB’s console makes monitoring very easy. The Home page enables the admin to see at a glance whether any clients require attention, and then easily find details of the problem. The ability to install missing updates directly from the computer’s details page is extremely convenient, and we wonder whether F-Secure might provide similarly convenient solutions for other problems, e.g. outdated signatures or deactivated protection components.

Managing the network

A scan can be run by selecting individual PCs from the Computers page using the checkboxes, clicking “Scan for malware” on the row of tabs above, and the “Assign operation” button. We could not find a means of running one-off updates or scheduling a scan from the console, although both these operations can be run from the client software on individual PCs. Components can be enabled or disabled from the Operations sub-tab on the Computers page:



When we tested the “Enable real-time scanning” function, the confirmation message from the console informed us that “The operation is completed within two hours”.

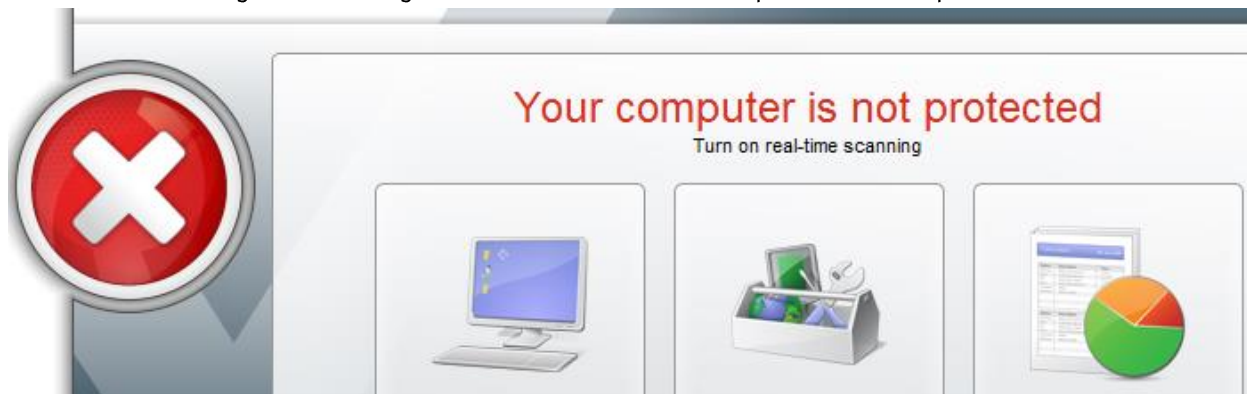
We found running a standard scan to be very easy, but wondered why updates and scheduled scans cannot be started in the same way. It strikes us that the system is quite slow in transmitting activation and status messages between the console and the clients, and wonder whether F-Secure might be able to improve this.

Client antivirus software

PSB Workstation Security installs a System Tray icon, which can be used to launch a variety of tasks. It registers with Windows Action Center as firewall, antivirus and antispyware. Windows Firewall is disabled; Windows Defender is disabled under Windows 8, but not under Windows 7. The main program window is fully featured and will appear very familiar to anyone who has used earlier versions of F-Secure’s consumer security software:

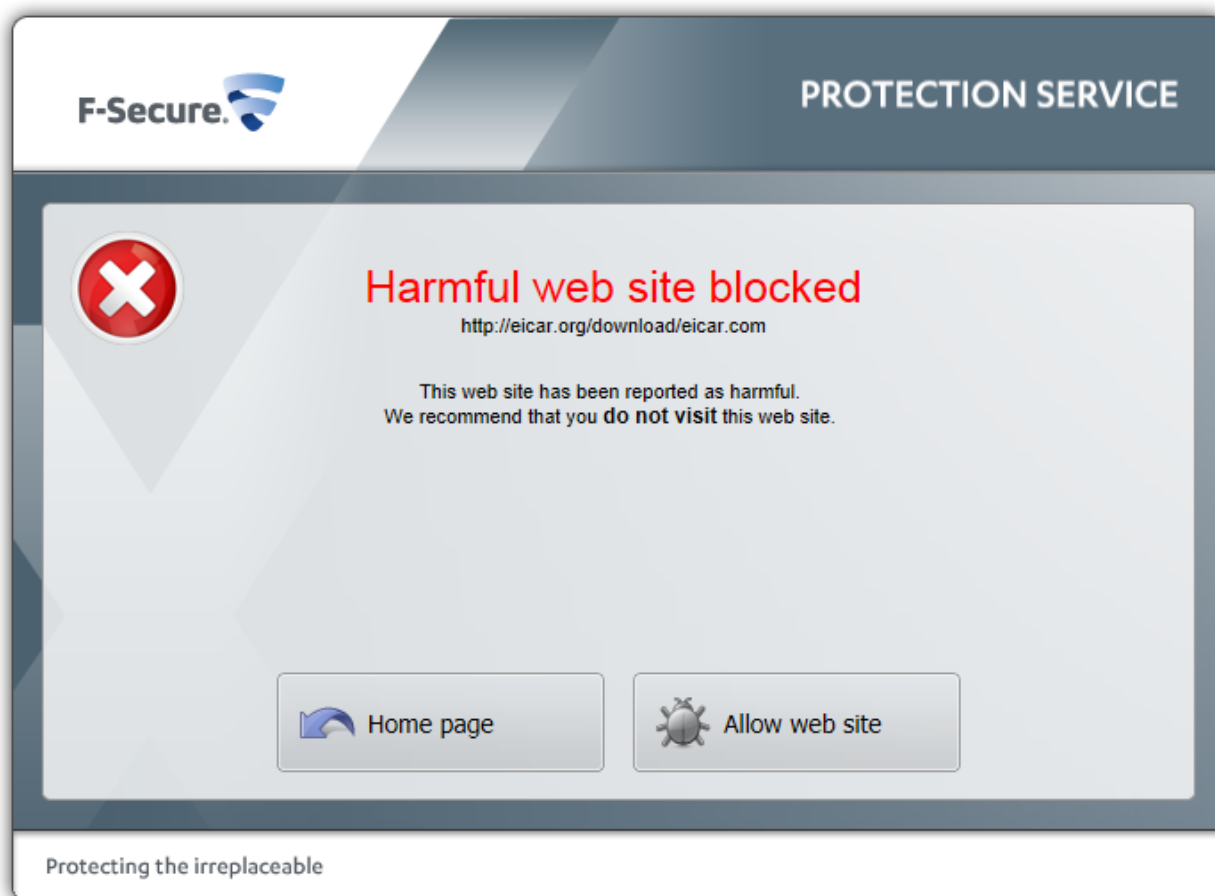


There is a status display in the form of a text heading and an icon. These are green when all is well, but turn red – along with a change in the text and icon – if a protection component is disabled:



There is however no means of reactivating the protection easily, an admin or user who sees such an alert has to go into the settings to enable the relevant component. By default, it is possible to disable the real-time protection without an administrator account; however, this can be blocked by the administrator via policy.

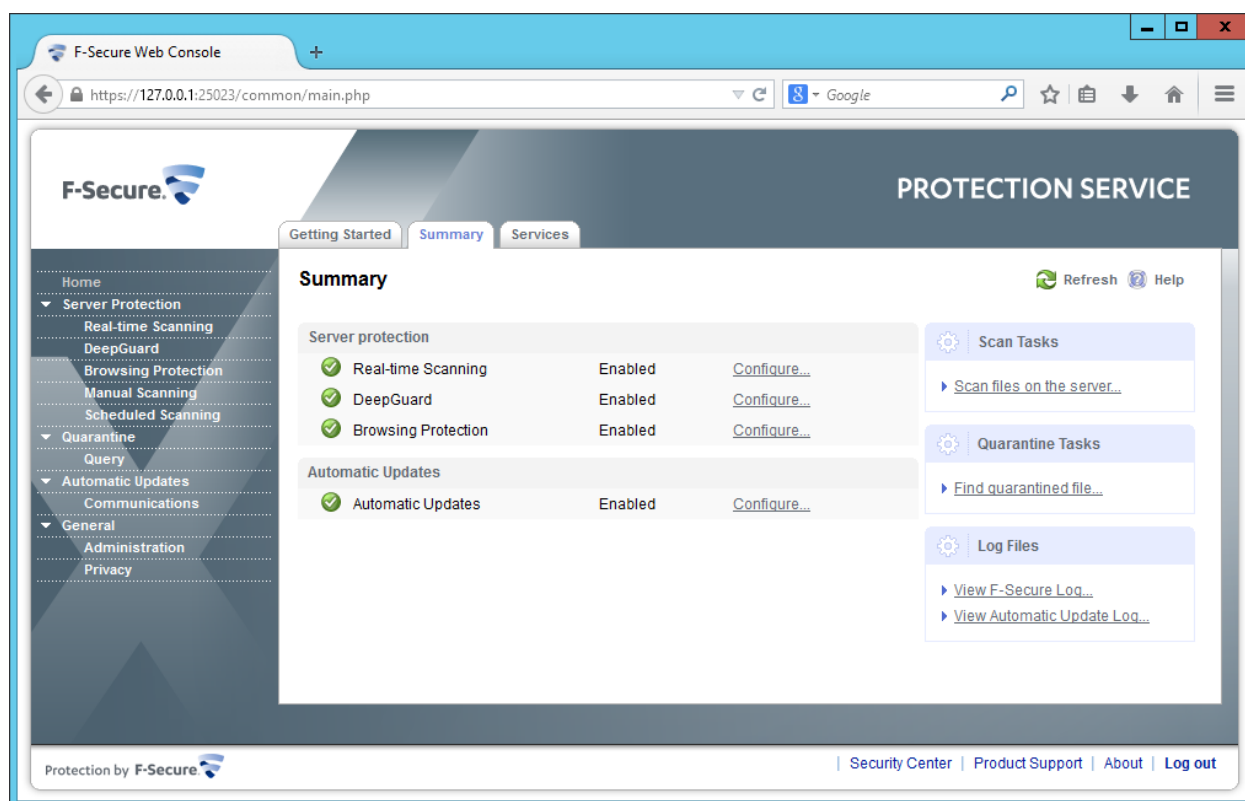
The following alert is shown if the EICAR test file is downloaded:



The client software has a simple and familiar design, and allows users to run scans and updates, which we find sensible. The malware warning is also very clear. However, we feel that the default policy should prevent standard users should from deactivating protection components. We also suggest implementing an easier way of reactivating protection (such as a fix-all button) in the event that it has been disabled.

Server antivirus software

The file-server protection software is a separate installation package, but can be downloaded from the console in just the same way as the client software. The setup wizard is very simple and does not require any specialist knowledge. The user interface is web-based, and so is accessed by typing the URL into a web browser. Instructions for this are included in the product manual (F-Secure E-mail and Server Security Administrator's Guide). As can be seen in the screenshot below, the interface has a status display and links to scans, quarantine, updates and settings:

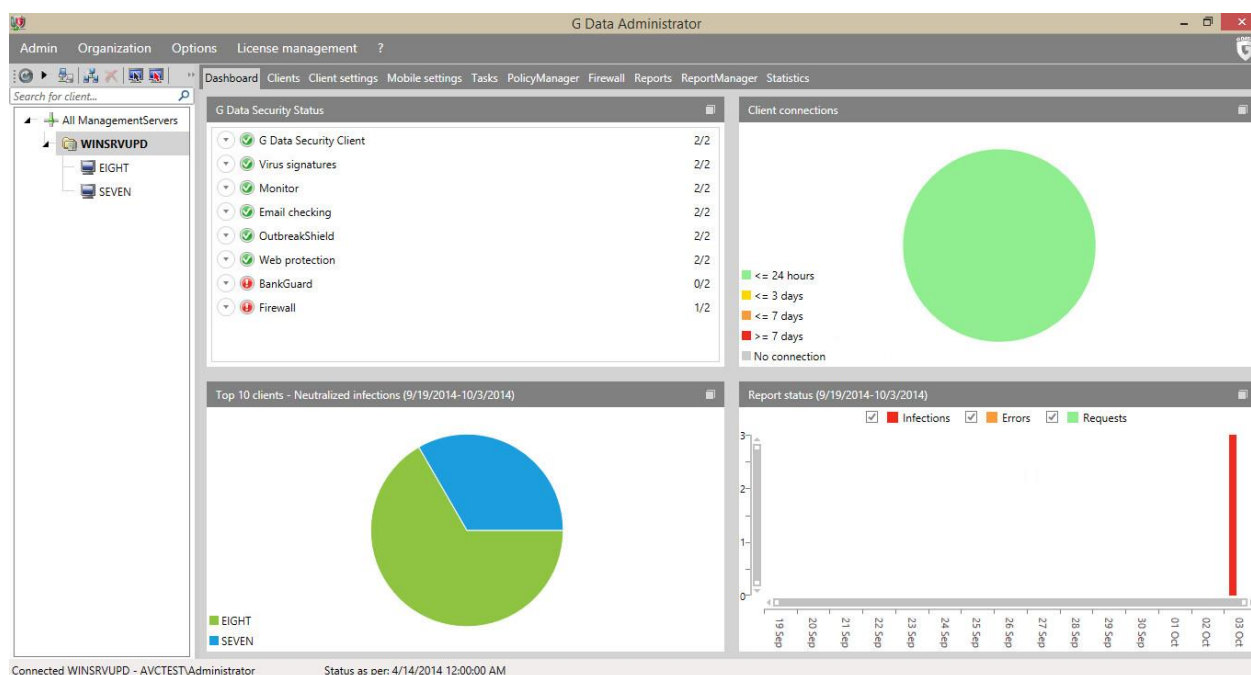


Inexperienced administrators might find it unusual to access an antivirus program via a web browser, but once the interface has been opened, it is actually not very different from the GUI of a consumer security product. With some help from the manual (which is produced to the same high standard as the console documentation), we feel that even non-expert admins should be able to manage the product without any difficulty.

Summary

F-Secure Protection Service for Business is extremely well suited to small businesses, including those without their own IT staff. The console is web-based and so requires no installation, while deploying the endpoint-protection software on client PCs is no more difficult than installing iTunes. The design of the console is very clean and simple, and it is easy to find details of any problems that have been noted on the overall status page. As the documentation is also very good, we feel that F-Secure PSB could be used successfully by small businesses without professional assistance being required. We have noted some minor suggestions for improvement, such as faster communication between console and clients, and minor modifications to the client software. However, overall we feel the product has been very well designed, and makes monitoring and managing a small-business network extremely easy.

G Data Antivirus Business



Introduction

G Data produce a line of business software with different packages according to business size and technical requirements. We have reviewed G Data Antivirus Business, which includes antivirus and firewall software for Windows clients and a management console. Features available in other packages include mobile device protection, antispam, mail security, client backup, patch management, and protection for Mac OS X.

Software version reviewed

G Data Administrator 13.0

G Data Security Client 13.0

System requirements

G Data Management Server runs on Windows Server 2003, 2008, 2008 R2, 2012, and 2012 R2, as well as the client operating systems Windows XP (32-bit only), Vista, 7 and 8. The G Data Security Client runs on all these systems, and also Windows 8.1.

Non-Windows platforms: Android 2.2 and above

Additional features

Client firewall, AntiSpam, BankGuard, Application Control, Device Control, Web Content Control, Internet Usage Control, Patch Management, Client Backup, MailSecurity, Report Management.

Documentation

The manual is included in the zip file that contains the software. It is 176 pages long, and covers all the functionality of the console, including managing email security and mobile software for Android. The installation of the console, along with deployment and management of Windows client software, are described in detail.

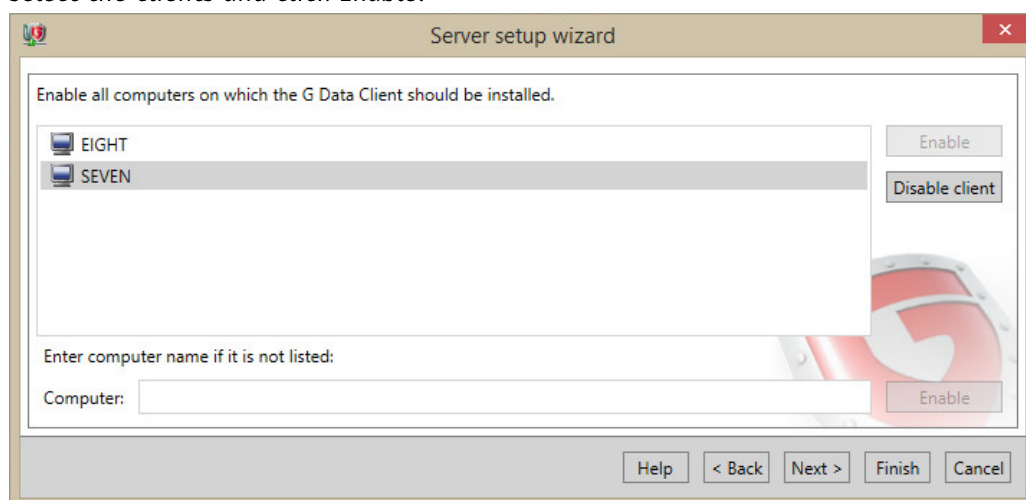
Packaging the documentation with the software strikes us as a simple but very useful idea. We found the manual to be comprehensive, clearly written and easily accessible through bookmarks and the hyperlinked contents page. It is also well illustrated with appropriate screenshots. There is also a local help service, which displays similar information to that found in the manual. We would describe the documentation overall as very good.

Preparing server and clients for deployment

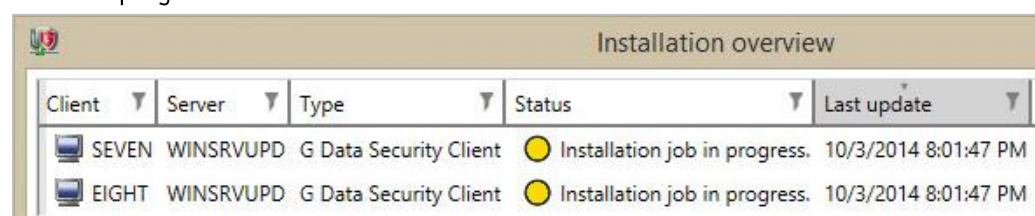
We enabled File Sharing and Network discovery on our client PCs, and were then able to deploy and manage the client software without any difficulty. We note that the manual recommends enabling the Remote Registry service, and disabling User Account Control and the File Sharing Wizard.

Deploying the software

The console is installed on the server by running a single installation file. This installs the management server and user interface together; the installer also provides the option of installing the user interface on additional computers. Microsoft SQL Server 2008 Express SP3 x86 is installed by default, although the user has the option of using an existing SQL Server installation instead. As soon as the console has been installed, the deployment wizard starts automatically. This immediately presents a list of client computers found on the network; the admin simply has to select the clients and click Enable:



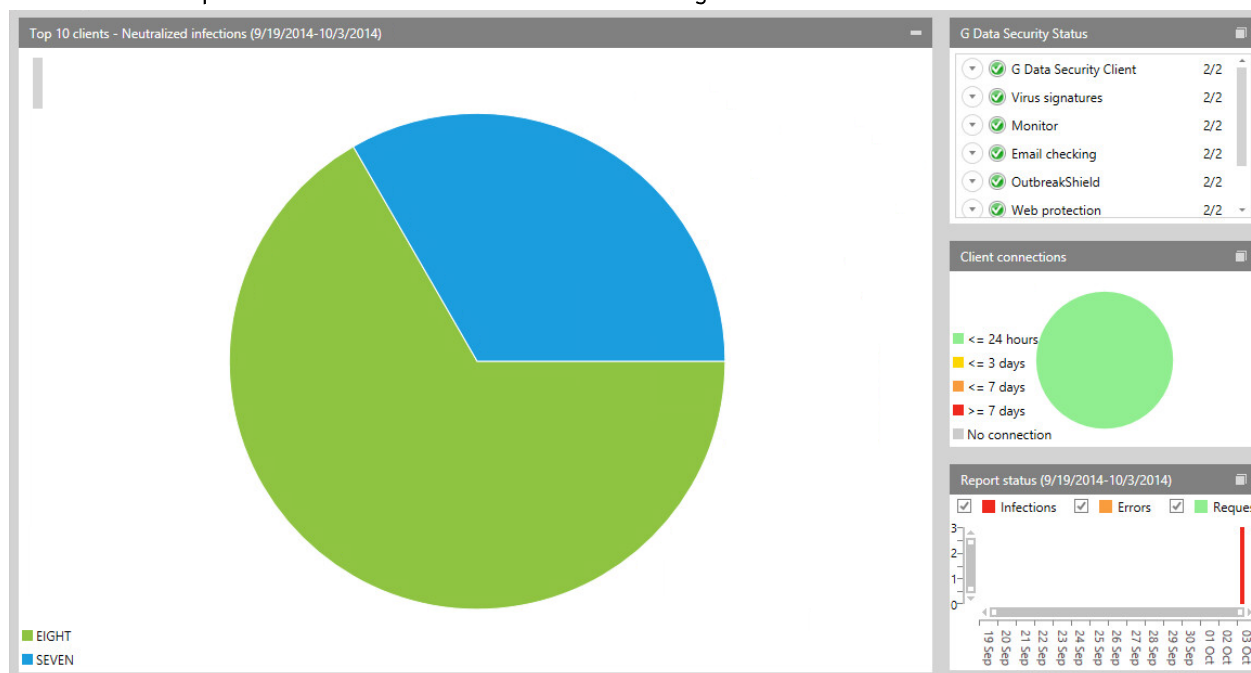
The username and password for the G Data licence then have to be entered, and an automatic update schedule set if desired. The admin can also set up email notifications for specific events such as virus finds, and choose a language for the client software interface. Installation then proceeds, with the progress shown in an overview window:



We found the installation of the console and subsequent deployment of the client software to be remarkably quick, easy and unproblematic. We feel that both stages are so straightforward that they could be carried out by a non-expert administrator, with assistance from the manual.

Management Console

The console has a narrow left-hand pane that shows the servers managed by the console. Clicking on the name of a server shows the client PCs it manages in a list underneath it. The larger right-hand pane shows by default the Dashboard, which consists of 4 panels, showing G Data Security Status, Client Connections, Neutralised Infections, and Report Status. A button in the top right-hand corner of each panel allows it to be maximised, whereby it expands to fill about three quarters of the pane, while the other panels are shown as thumbnails on the right-hand side:



A row of tabs along the top of the main pane allows different pages to be displayed, including a detailed list of individual clients and their status, client settings, and tasks.

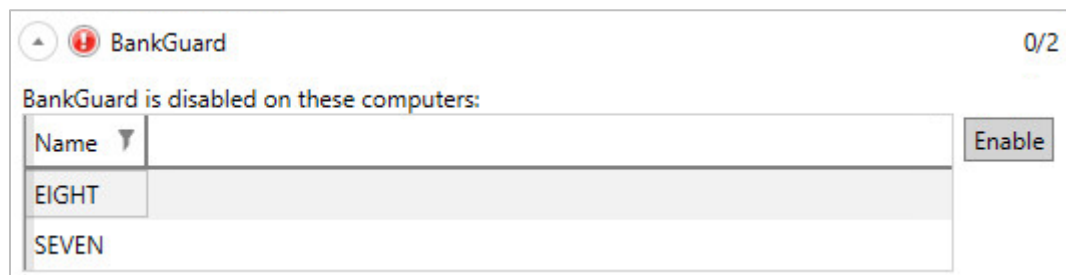
We found navigating the console to be particularly easy, as all the available pages are shown in one menu bar along the top of the window. The ability to maximise one panel of the dashboard with a single click is very convenient.

Monitoring the network

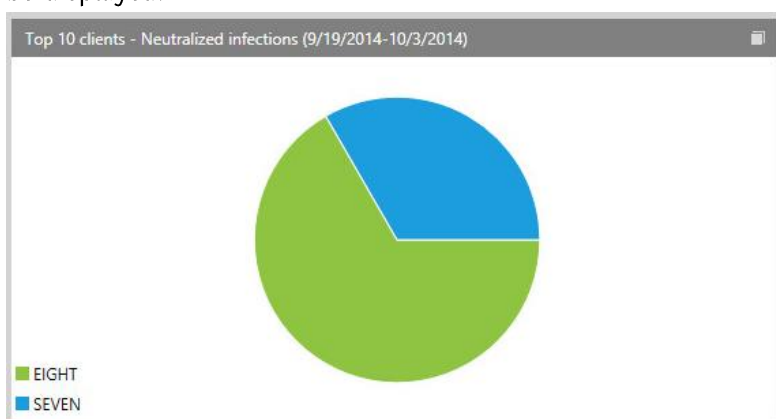
The G Data Security Status panel of the Dashboard (home page of the console) shows a detailed report of the security status of client computers, broken down into elements such as Virus Signatures, Monitor (real-time protection), Web Protection, and Firewall. If the component is working properly on all clients, the status icon shows a tick in a green circle; if there is a problem with any individual client, the icon shows an exclamation mark in a red circle, with the number of affected clients shown at the end of the line:



Clicking on an item showing a problem displays a list of the computers affected, along with a button for rectifying the problem. In the example below, the Bank Guard component is disabled on 2 computers. To resolve the issue, the administrator just needs to select the computers by clicking on them, and then click Enable:



Malware finds are shown in the Neutralized Infections panel of the Dashboard, in a pie chart divided up by client PCs affected. Clicking the calendar symbol (which appears when the mouse pointer is moved over the Maximise button) allows the admin to set the date range for which infections are to be displayed.



The Clients tab of the console displays the precise version of the G Data Security Client running on each client PC, along with signature versions for both antivirus engines used. Licensing information can be found by clicking the License Management menu at the very top of the window.

The client status panel strikes us as a very simple but effective way of displaying the security status of all the computers on the network. The ease with which the administrator can find computers showing a problem, and immediately put this right from the same panel, is outstanding.

Managing the network

Single scans can be run for the entire network by clicking the server in the left-hand pane of the console, then Tasks, and the Single Scan Job icon. Running a scan job on a single computer is the same, except that the admin just needs to click the individual client in the left-hand pane, instead of the server. There is also a Periodic Scan Job icon under Tasks, which can be used to set scheduled scans.

Updates can be run from the Clients tab, by selecting the computer(s) concerned, right-clicking, and selecting "Update virus signatures now" from the context menu.

Running updates and scans from the G Data console struck us as intuitive and unproblematic.

Client antivirus software

The G Data Security Client registers with Windows Action Center as antivirus and antispyware, and also firewall if the admin chooses to install this component. Windows Defender is disabled under Windows 8 but not Windows 7. A System Tray icon is installed. The context menu shown when this is right-clicked represents the entire user interface of the client software. By default, the only action the user can carry out is to run an update:



This can be extended by the admin from the console, to include scanning and monitoring options. If the EICAR test file is downloaded, an alert page is shown in the browser window:



The minimalist interface to the client software may come as a surprise to some administrators, but prevents users from disabling the protection or being distracted by complicated alerts. The functions available can be extended very quickly and easily from the console if necessary, so that e.g. scans can be run locally.

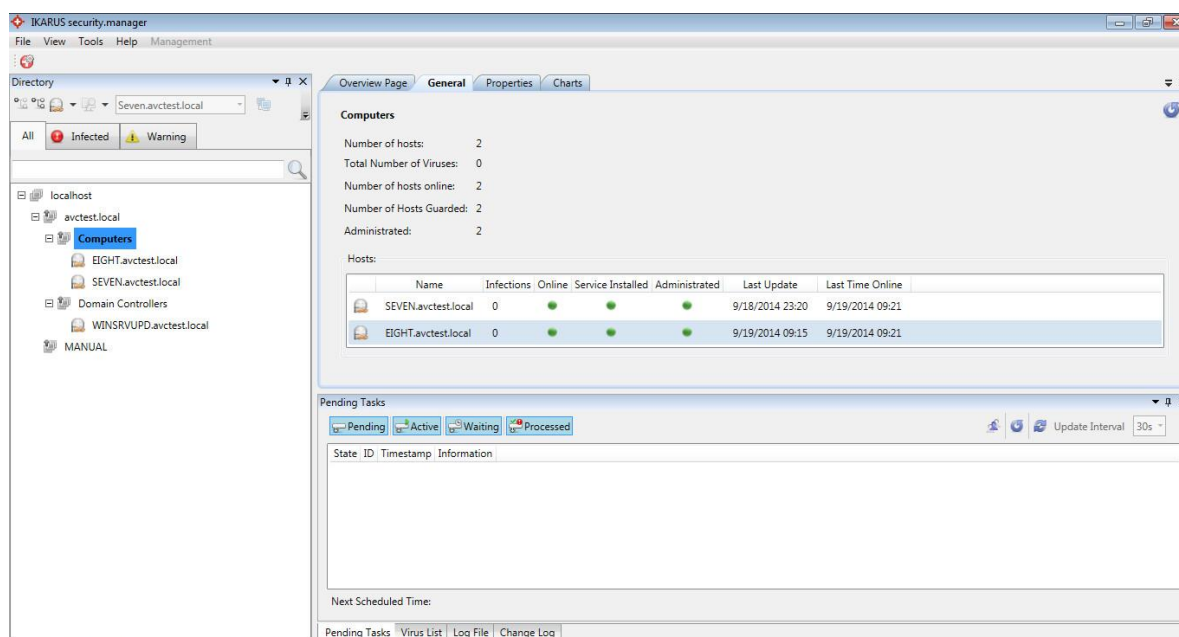
Server antivirus software

This is identical to the client software in terms of installation, interface and the way it is managed in the console.

Summary

We found G Data Antivirus Business to be exceptionally easy to set up and use. It is one of the most user-friendly server consoles we have encountered, and we feel that even non-expert administrators should be able to install and use it, with some assistance from the manual. Outstanding features include the extremely easy client-software deployment, and the very convenient means of rectifying problems directly from the status display panel of the console. We would suggest the product is ideal for a company of 20 to 25 users, as it provides all the functionality of a traditional server-based console without requiring a full-time system administrator to manage it. Documentation is also very good.

IKARUS security.manager



Introduction

IKARUS produce endpoint protection for Windows and Android, gateway protection products, and cloud-security services for mail and web. For this review, we tested IKARUS anti.virus endpoint protection software, managed by the IKARUS security.manager console.

Software version reviewed

IKARUS security.manager 4.2.43

IKARUS anti.virus 2.7.30

Supported operating systems

The IKARUS security.manager console runs on Windows Server 2003 and 2008, both as 32 and 64-bit variants; also Windows Server 2008 R2 and 2012, 64-bit only. The anti.virus endpoint protection software is supported on Windows Vista and Windows 7, both 32 and 64-bit architectures.

Documentation

There are separate manuals for the antivirus software and the console. The manual for anti.virus is very comprehensive at 71 pages, and covers all aspects of installing, configuring and using the product. The layout and formatting are simple, but combined with very generous use of screenshots, this makes the document very easy to read. A clickable contents page enables easy access to particular sections. The manual for the console is also extensive at 120 pages, very detailed, and includes a glossary of terms. It is produced to the same high standard as the client-software manual.

Overall we would say the documentation is very good. We particularly liked the simple layout of the manuals and abundant screenshots, which we found made it very easy to read.

Preparing server and clients for deployment

We enabled file sharing and network discovery on the client PCs, and this was all that was necessary. Two ports need to be opened on the server firewall to allow communication; these are noted in the manual.

Deploying the software

There are two separate components to install for the console, namely the server and the UI. The server component requires Microsoft SQL Server Express; there is a link to download this in the wizard. The admin can pause the IKARUS setup, install SQL Server, and then continue with the IKARUS wizard from the point he/she left off. Installation of the UI component is very quick and simple.

Once the console is up and running, it can be used to deploy the anti.virus software to the clients. This is done by right-clicking a computer or group of computers and selecting "Install IKARUS anti.virus":



We would definitely recommend that the console should be installed on the server by an IT professional. Although it could not be described as difficult, some of the tasks, such as installing Microsoft SQL Server or creating file shares, require some expertise. However, the deployment of the endpoint protection software to the clients could not be simpler, and so a non-expert could easily add the protection to new client machines the network.

Management Console

The design of the security.manager console is quite straightforward. There is a narrow left-hand pane displaying the computers on the network, in Active Directory groups, i.e. domain, Computers OU and Domain Controllers OU. Two horizontal panes on the right show detailed information about the group or computer selected, such as details of status, pending tasks, or malware found. The relative size of the panes can be customised by drag and drop, or one pane can be closed altogether.

The console has a fairly standard structure, not unlike the Microsoft MMC, and we would say that with a little bit of exploration it is reasonably easy to find one's way around.

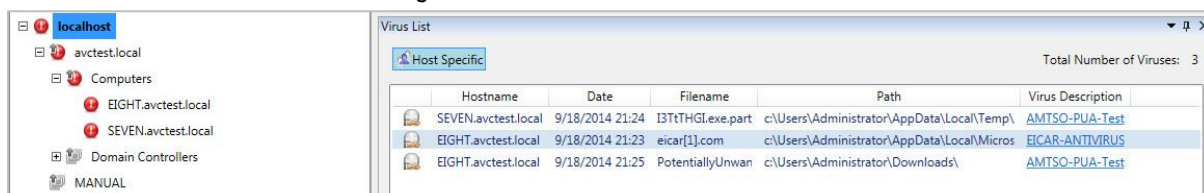
Monitoring the network

The General tab at the top of the right-hand pane of the console shows the status for individual client PCs or groups (up to and including the domain). Clicking on a client in the left-hand pane, then clicking the General tab in the right-hand pane shows detailed information about the system in question, including software version, signature version, licence information, protection components enabled, infections, times of next and last scans, and more. Information for groups is (inevitably) more limited, and does not include the status of real-time protection.

The information displayed for individual PCs is very comprehensive. However, we feel that real-time protection should be amongst the items displayed for all computers in a group, so that the administrator can easily see that it is running on all clients. This could be done by changing the computer's icon in the left-hand pane, which would not require any more space to display the warning.

There is a refresh button in the top right-hand corner of the General page, which allows admins to see status changes immediately.

If malware is detected on client computers, those affected will be shown in the left-hand pane of the console with a red icon bearing an exclamation mark:



The Virus List tab of the right-hand pane shows the individual files affecting each computer. If an individual computer is selected, the “Purge System” button at the bottom of the console becomes active, and clicking it clears the list of malware items for that computer.

In our test, it was not entirely clear to us what the “Purge system” button actually does. The manual states that it “Deletes the selected infections of the list”, which we also find rather confusing. In fact, the files are held in the client's local quarantine, which is emptied by clicking “Purge System”. We suggest that “Empty Quarantine” would be a much clearer description.

Managing the network

An individual computer can be scanned by selecting it in the left-hand pane and clicking the scan icon at the top of the pane. Groups can be scanned by creating configurations from the IKARUS icon just below the menu bar. A configuration includes all possible client settings, along with scan types and schedule. Updates can be run on individual clients or groups by right-clicking and selecting “Update IKARUS anti.virus”.

We suggest that adding one or more scan entries to the right-click menu for groups would enable the admin to scan multiple computers with just one click, which would be very convenient.

Monitoring and management using replica of client window

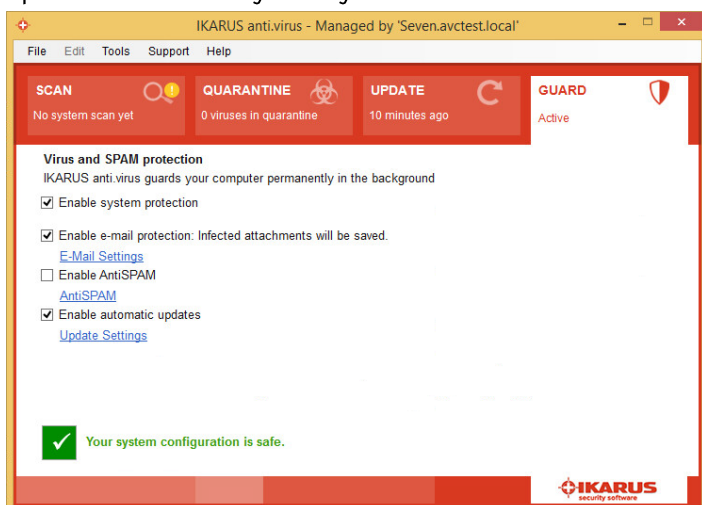
A feature of the security.manager console is the ability to display a replica of the client software window from the console. By right-clicking a client PC in the left-hand pane of the console, and then selecting “Start IKARUS anti.virus”, the administrator can display the client software window exactly as it would be shown on the PC itself, and carry out all tasks such as running updates or scans, enabling or disabling components, and checking the quarantine that are normally available from the anti.virus client window.

We feel the replica of the client window is a very innovative idea, and one which would make it very easy for new admins to start monitoring and maintaining individual PCs.

Client antivirus software

IKARUS anti.virus registers with Windows Action Center as antivirus and antispyware. Windows Defender is disabled in Windows 8, but not in Windows 7. There is a System Tray icon, which can be used to open the program, run updates, and switch protection on or off.

The main program window of anti.virus is graphically very simple, but displays status, scan and update functions very clearly:



If system protection is disabled, the status display changes accordingly:



As the protection can be reactivated from the checkbox on the home page, there is no need for a Fix All button. We found that by default it is possible to disable the protection using a non-administrator account; however, the admin can configure the software to restrict this. When the EICAR test file is downloaded, the alert below is displayed, but this can be disabled from the console if desired.



The main program window of the client software makes the essential functions easily accessible, and displays the status clearly. We suggest that supressing that admins may want to configure the system to block the malware alerts (which we found rather alarming), and prevent standard users disabling protection components.

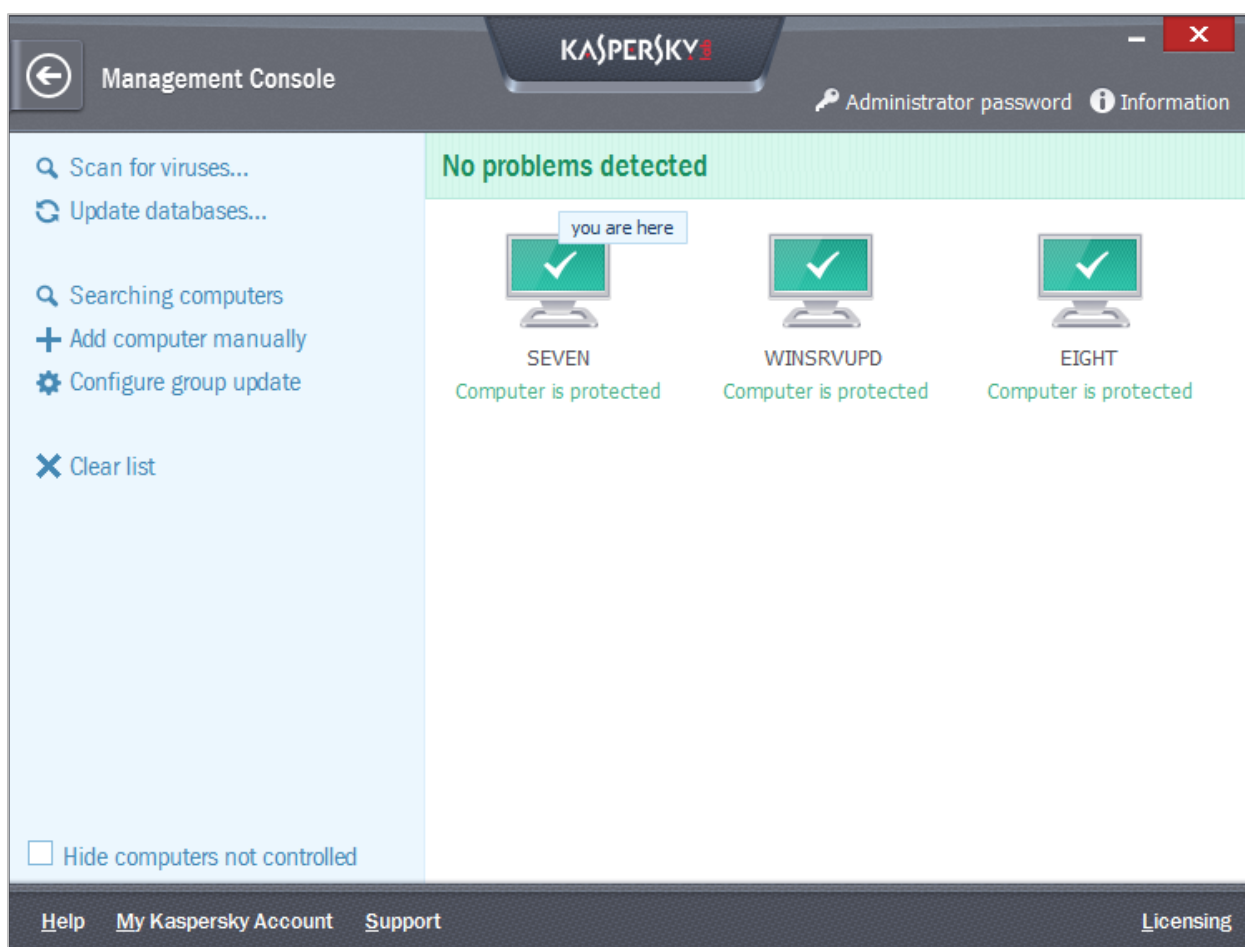
Server antivirus software

This is identical to the client software.

Summary

We would definitely recommend small businesses using IKARUS security.manager to have an IT professional install and configure the software, and train staff in its use. Monitoring and maintaining the network should then be quite straightforward for non-expert administrators. Some features of the software are excellent, such as the ultra-simple push installation of client PCs, and the replica client-software window, which we feel is ideal for inexperienced admins. The two manuals, for the console and client respectively, are clear, detailed and easy to read. We do have a couple of suggestions for improvement, however: showing real-time protection for all clients in one window, and making malware detection alerts less alarming to the user.

Kaspersky Small Office Security



Introduction

Kaspersky Lab's main line of business products is called Kaspersky Endpoint Security for Business. This is scalable for networks of 10 client PCs upwards, with components for client PCs (Windows, Mac and Linux), Servers (Windows and Linux), mobile devices (Windows, Android and iOS), and a separate, server-based management console. We covered this product in our Business Review October 2013 (<http://www.av-comparatives.org/corporate-reviews/>).

For small businesses with up to 25 PCs, Kaspersky Lab has a tailor-made product called Small Office Security, which we have reviewed here. It features Windows client software with integrated console, and protection for Android mobile devices (the latter is not covered by the review).

Software version reviewed

Kaspersky Small Office Security 13.0.4.233a

Supported operating systems

Windows XP 32-bit; Windows Vista, 7, 8, 8.1, all 32 or 64-bit

Windows Server 2008 R2, 2012; Windows Small Business Server 2008, 2011

Android 2.3 – 4.3

Additional features

Client firewall, Rescue Disk, File Shredder, Password Manager, Data Encryption, Safe Money, Backup, Web Policy Management, Virtual Keyboard. According to Kaspersky Lab, SafeMoney protects financial

operations via online banking, payment systems such as PayPal, and e-shops. Virtual Keyboard displays a software keyboard on the screen, which can be used to enter sensitive data such as passwords, with the aim of preventing a keylogger being able to capture this.

Documentation

There is a 78-page manual for the product, which can be downloaded from the same page as the software. The manual covers all aspects of installation, configuration and use of the product. It has been fully indexed and bookmarked, and is illustrated with screenshots where applicable. There is also an online knowledge base, which again provides instructions for all aspects of using the product, with a menu panel on the left-hand side of the page acting as a clickable index. Where appropriate, there are screenshots and even videos to illustrate the articles.

We found Kaspersky Lab's help facilities to be outstanding. Both the manual and the knowledge base provide comprehensive coverage, which is clearly written, well-illustrated, and easily accessible.

Preparing server and clients for deployment

We found that it was necessary to enable Network Discovery and File Sharing on all computers to enable communication with the console. We could not find any reference to this in the manual.

Deploying the software

There is a single 186-MB setup file, which is used to perform a local installation on each computer (server or workstation) on the network. Installation requires literally one double click and two single clicks. Once the setup file has been executed, clicking the Install button will complete the process:

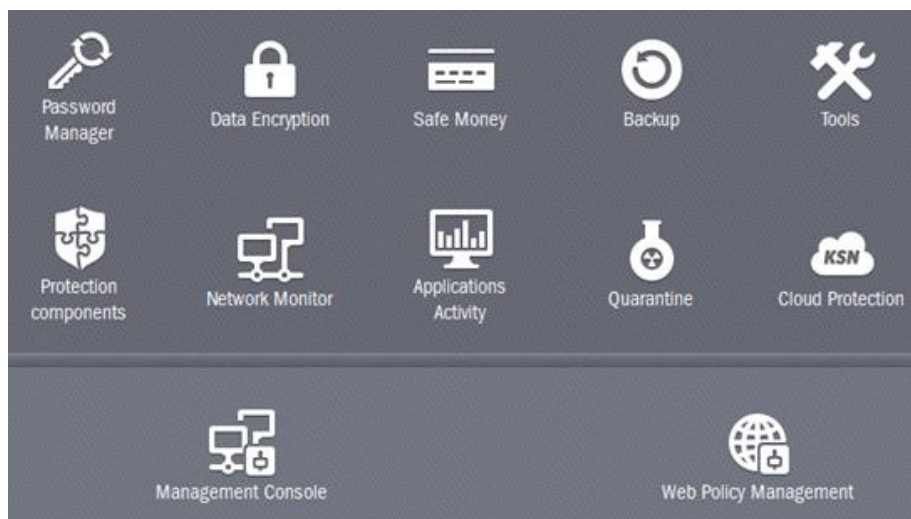


The only option is to join the Kaspersky Security Network (data-sharing scheme). The setup program initially searches for any newer version of the software, even though it is self-contained and could even be installed offline.

We would say that anyone who can install a consumer version of Kaspersky Lab software can also install Small Office Security, that is to say, an IT professional is not required. We like the fact that the setup program is self-contained, but searches for a newer version as well.

Management Console

The management console does not run in its own window, but is integrated into the client antivirus interface. Clicking on the "up" arrow in the bottom right-hand corner of the client window shows the full range of tools, and access to the console:

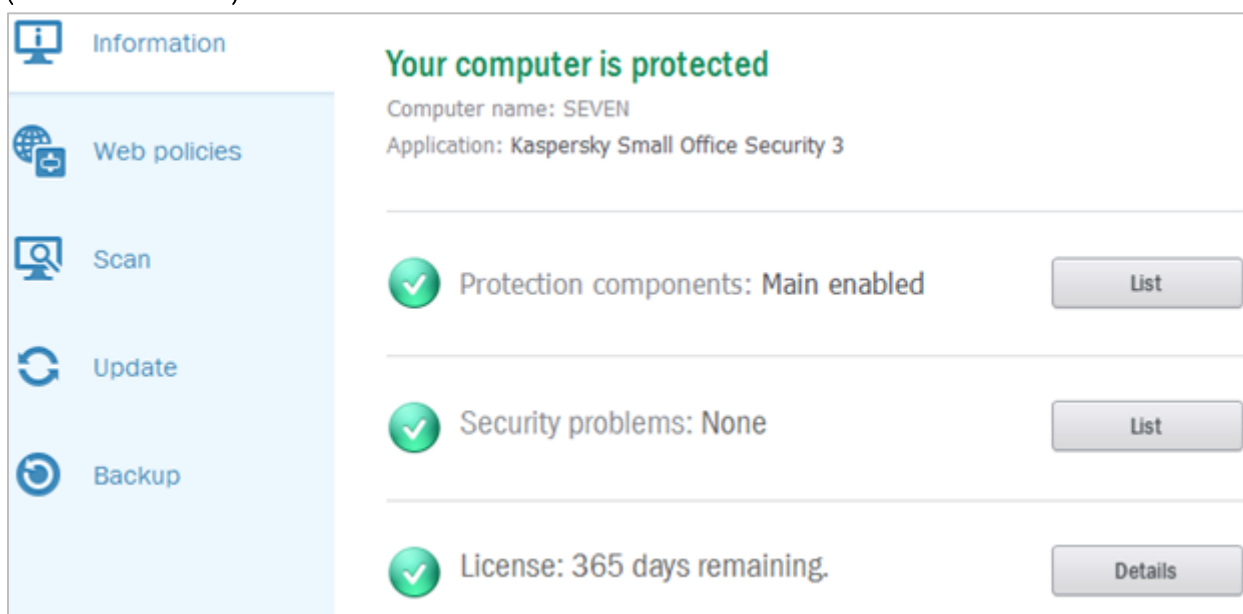


The first time the administrator opens the console, a password has to be created, which prevents unauthorised access to the console or settings. The console is then displayed; this is shown in the main picture at the beginning of this report. The larger right-hand pane displays the computers on the network, and their status. A menu panel on the left-hand side allows scans and updates, and options for adding computers.

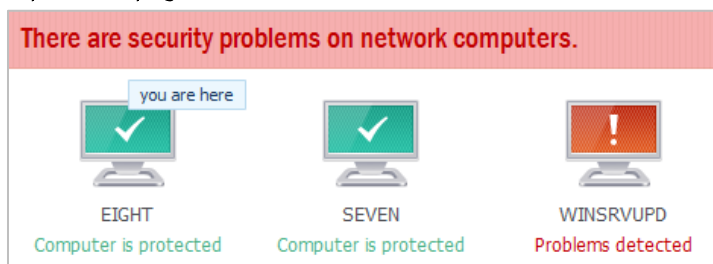
The integration of the console into the client antivirus window strikes us as ingenious. It allows the network to be managed from any client or server computer. We found the overview of network computers, along with status display and scan/update functions, to be a model of simplicity and clarity. Altogether, we feel the console design is outstanding for non-expert administrators who may be managing network antivirus for the first time, and that even experienced IT staff would appreciate the ease of use.

Monitoring the network

The “Computer is protected” status indicates that major protection components, including real-time protection and firewall, are working properly, and that the malware signatures are up to date. Clicking on the icon for a particular computer shows a more detailed status report for it (“Information” tab):



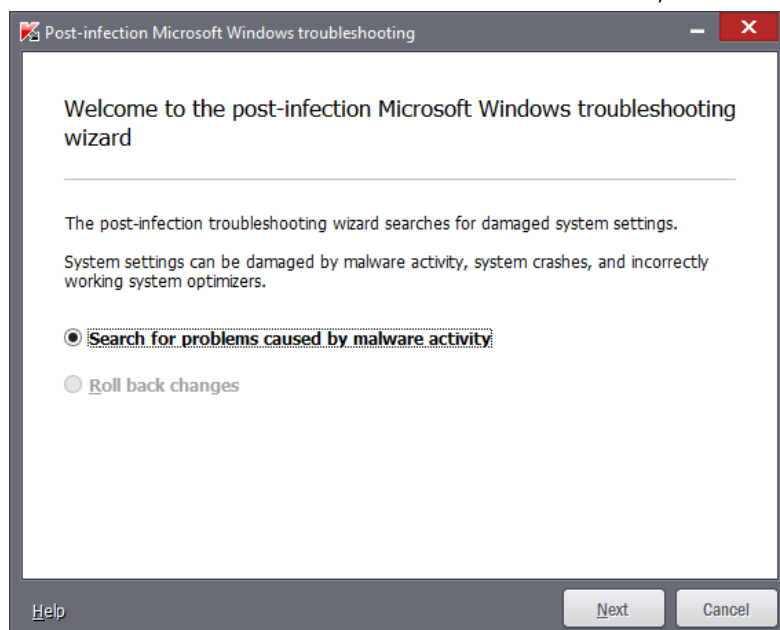
If there is a problem with a particular computer, the green-coloured text/icon on the console main page turns red, and the status display changes to “Problems detected”, along with a warning at the top of the page:



The detailed status page for that computer then shows the nature of the problem, and how to rectify it:



When we downloaded the EICAR test file on a client, we found that it was deleted locally by the Kaspersky Small Office Security client, and the status in the console did not change. However, when we did the same with the AMTSO Potentially Unwanted Application, the computer’s status icon in the console changed to yellow, with the text “Problems detected”. Clicking on the icon opened the computer’s Information page, from which we had a choice of deleting or keeping the application. We noted that on the client where the detection occurred, a clean-up wizard is run:



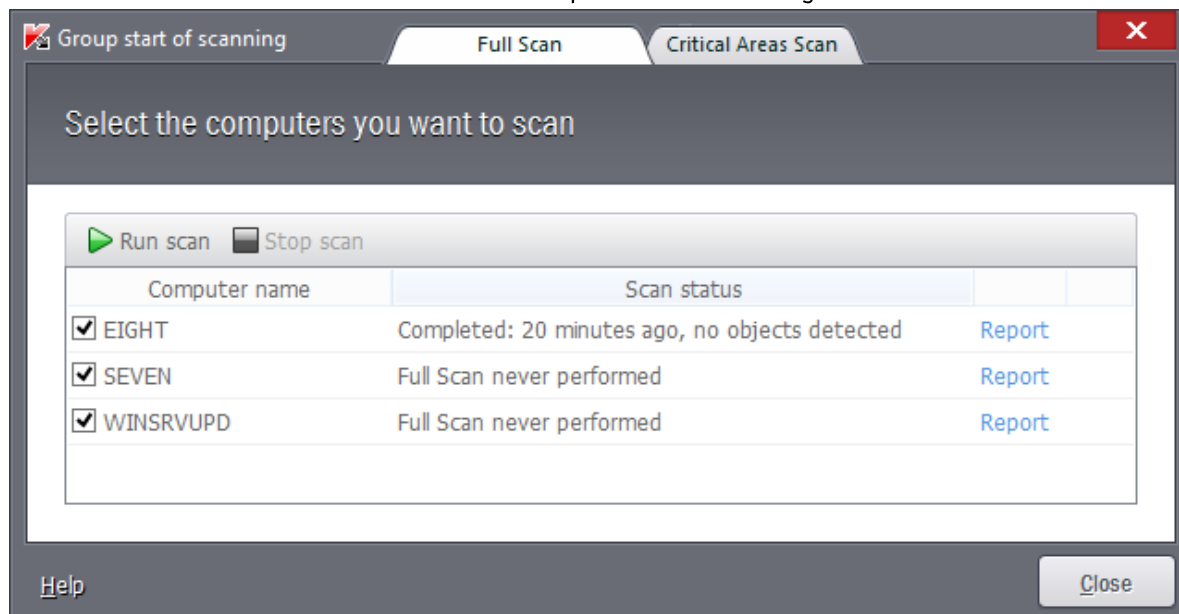
If this is run, it recommends any necessary action to clean up the computer or improve security generally.

Licensing information is displayed on the Information page for each individual computer (please see earlier screenshot). We could not find a means of displaying the current program version in the console, although we feel this should not be a problem in a small office.

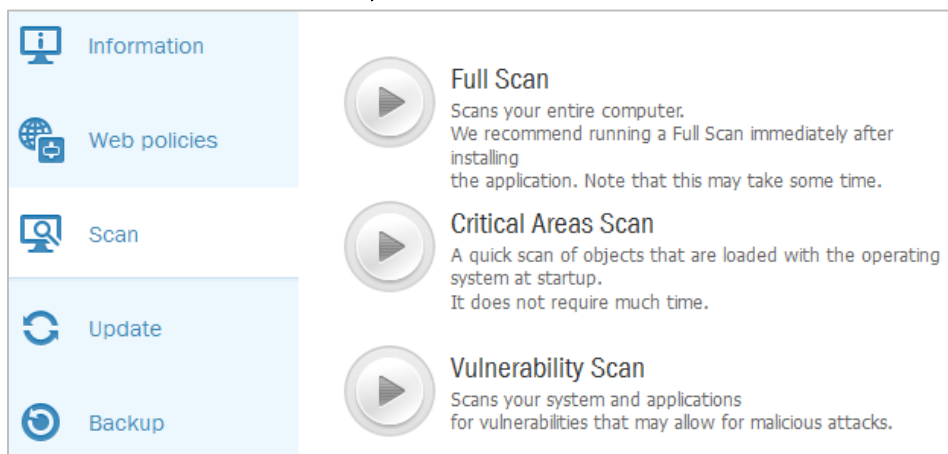
We found the method of dealing with malware/PUAs to be very appropriate for a small office network, and the Post-Infection Wizard is a good way of ensuring the system is secure.

Managing the network

Malware scans can be run on multiple computers by clicking the “Scan for viruses” link in the top left-hand corner of the console window. This opens the scan dialog box shown below:



By default, all computers are selected, though it is easy to deselect individual machines by clearing the appropriate check boxes. There is a choice of Full or Critical Areas scans. Updates for multiple computers are run by clicking “Update databases” in the console home page; a dialog box very similar to the one allows any or all computers to be selected. It is also possible to run updates and scans on an individual computer by opening its Information page and clicking “Update” or “Scan” as appropriate. The Scan page provides three options, namely Full, Critical Areas, and Vulnerability. Each one has a succinct description:



We could not find a means of running a scheduled scan, but we note that the Idle Scan is enabled by default; this starts a scan when the computer has not been used for 5 minutes. Although an update schedule cannot be configured for all computers from the console, it is possible to change the schedule for one computer and then use this to distribute updates to the rest (using “Configure group update” from the menu panel in the console home page).

We regard updates and scans as the two most important network tasks for the administrator, and we feel Kaspersky Small Office Security makes it extremely easy to carry them out, even for non-expert administrators.

Client antivirus software

Kaspersky Small Office Security registers with Windows Action Center as antivirus, antispyware and firewall, and there is a system tray icon. Windows Firewall is disabled. Windows Defender on Windows 8 (full antivirus program) is disabled, but Windows Defender on Windows 7 (antispyware only) it is not. A full user interface is shown, including status display, update and scan functions:



If a protection component is disabled, the status display warns of this and provides a “Fix” button to rectify the problem:



Administrator credentials have to be entered to disable protection, so this cannot be done by a standard user. When the EICAR test file is accessed, the following alert is shown, and remains until closed:



We regard Kaspersky Lab's client software as very appropriate for a small office. The interface is very clearly laid out and displays useful functions and information. A standard user can see the status and run updates and scans, but not disable protection or access the console, which we find ideal. The simple and familiar design, very similar to Kaspersky Lab's consumer products, should help non-expert administrators find their way around the product easily.

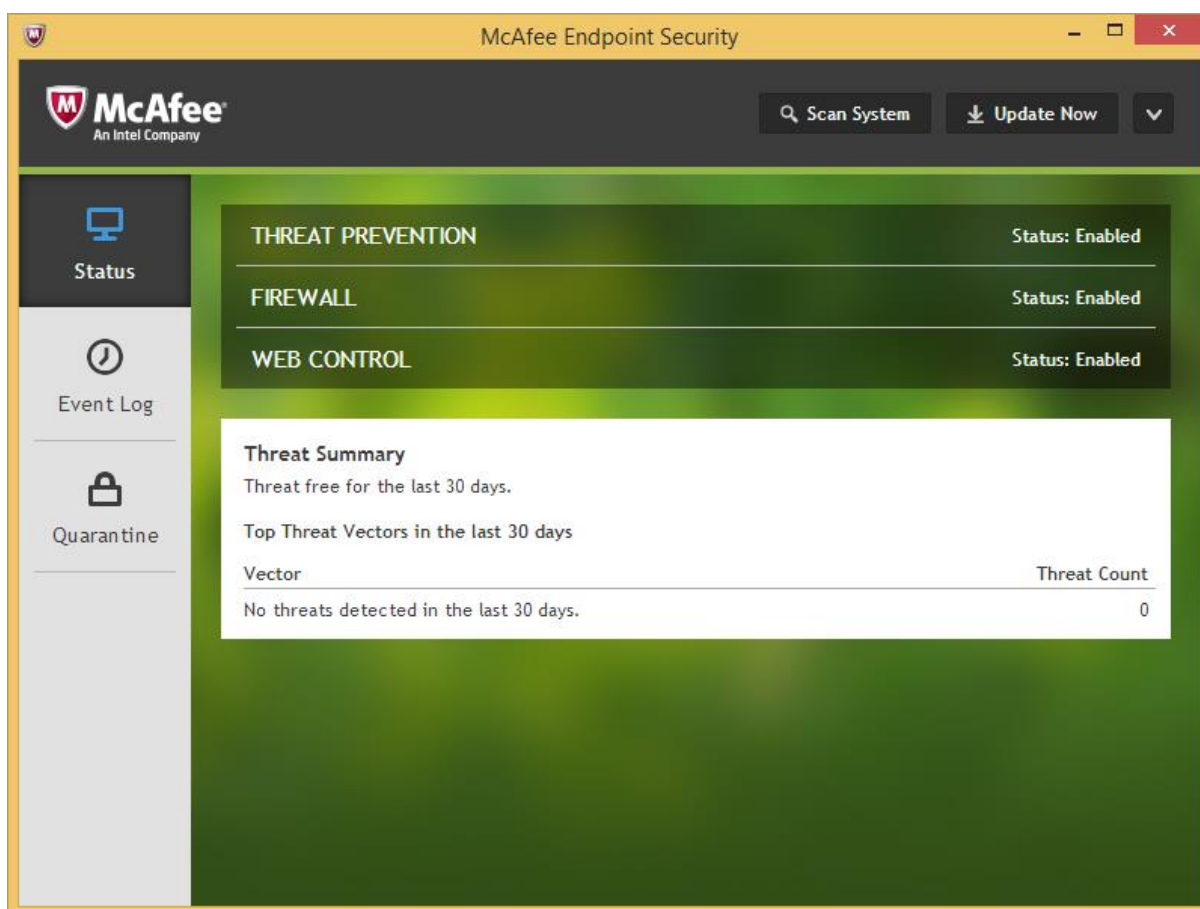
Server antivirus software

This is installed from the same installer file as the client software, and is largely identical. A slightly different selection of tools is shown along the bottom of the window, and the firewall is not enabled by default.

Summary

Kaspersky Small Office Security is aimed at small businesses with up to 25 PCs, and we feel it is extremely well suited to such a network. Integrating the console into the client software strikes us as a very clever idea, which should help to make life simple for non-expert administrators. Deploying the software is as easy as installing iTunes, so professional assistance should not be required. The management interface does not overwhelm the user with features, but makes the important functions – status monitoring, updates and scans – very easy to access. The manual and online knowledge base are up to Kaspersky Lab's usual excellent standard.

McAfee Endpoint Security (Self-Managed Option)



Introduction

McAfee Endpoint Security is endpoint protection software for business, with a number of different management solutions, as shown below:

Management type	Description
McAfee ePolicy Orchestrator	An administrator manages Endpoint Security using McAfee ePO (on-premise).
McAfee ePolicy Orchestrator Cloud	An administrator manages Endpoint Security using McAfee ePO Cloud.
McAfee SecurityCenter	An administrator manages Endpoint Security using SecurityCenter.
Self-Managed	Endpoint Security is managed locally using Endpoint Security Client. This mode is also called <i>unmanaged or standalone</i> .

Administrators can choose an option that is suitable for the size and complexity of their respective networks, as well as their own preferred management methods. This review covers the “Self-Managed” option, particularly suitable for small networks, in which the software is managed locally on each machine from the client interface.

We reviewed the McAfee Security Center in our 2012 Business Software Review (<http://www.av-comparatives.org/corporate-reviews/>).

Software version reviewed

McAfee Endpoint Security 10.0

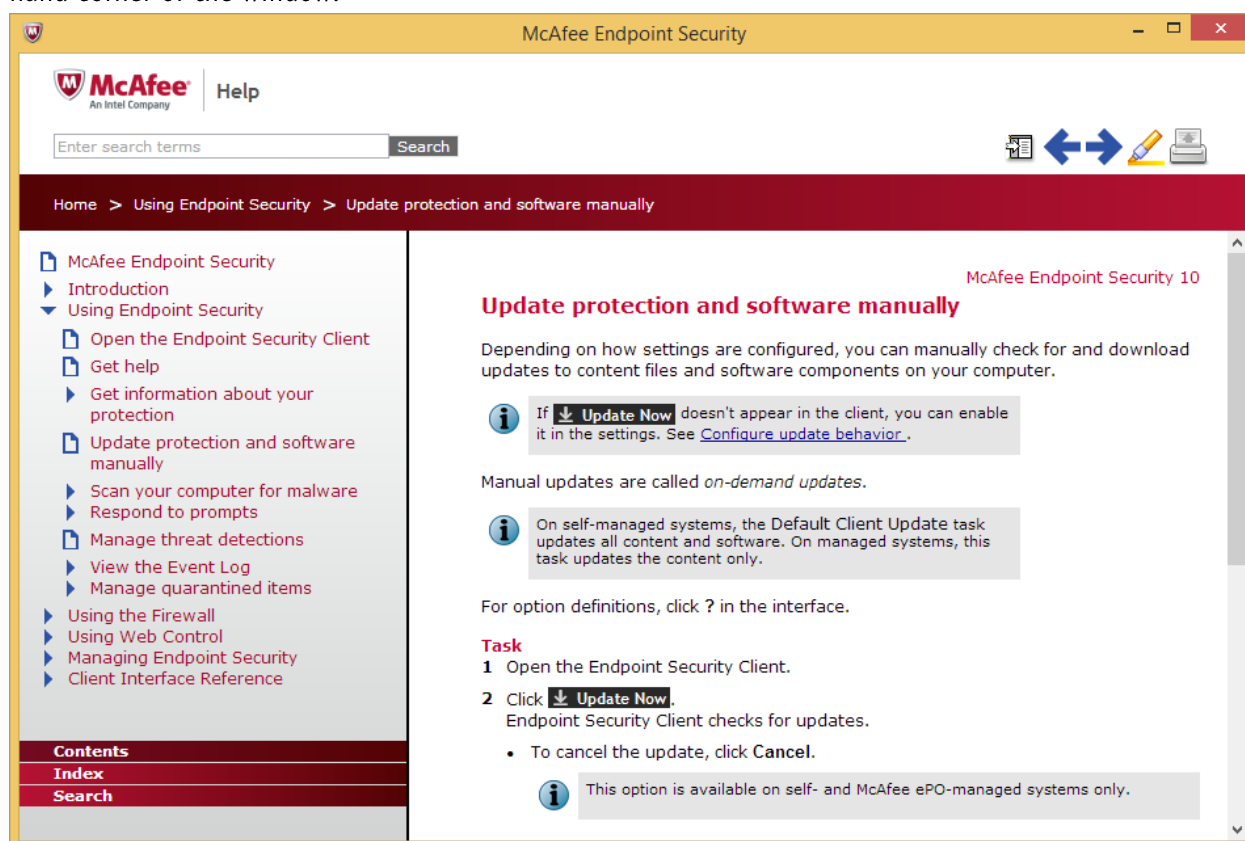
Supported Operating Systems

Windows Client Operating Systems: Windows 8.1 Update1, 8.1, 8 (not including RT), 7, Vista, 32-bit XP SP3 Professional ; Embedded for Point of Service (WEPOS), Embedded 8 (Pro, Standard, Industry) Embedded Standard 7;

Windows Server Operating Systems: Windows Server 2012 R2 Essentials/Standard/Datacenter (including Server Core mode); 2012 Essentials/Standard/Datacenter (including Server Core mode); Windows Storage Server 2008 and 2008 R2; Windows Small Business Server 2011, 2008, 2003 and 2003 R2; Windows Embedded Standard 2009; Windows Point of Service 1.1; Windows Point of Service Ready 2009

Documentation

There is a comprehensive local help feature, accessible from the drop-down menu in the top right-hand corner of the window:



The left-hand pane of the window shows a list of topics and sub-topics which can be displayed in the larger right-hand pane. There are no actual screenshots, but graphics of the individual controls, such as the Update Now button and drop-down menu button, are included. There is a search box at the top of the window.

We found the local help feature for McAfee Endpoint Security to be appropriately comprehensive, well laid-out and easily accessible. The texts are clear and succinct, and the search function works well, finding relevant articles for each search term. We would say that it is ideal for helping the administrator manage the product locally.

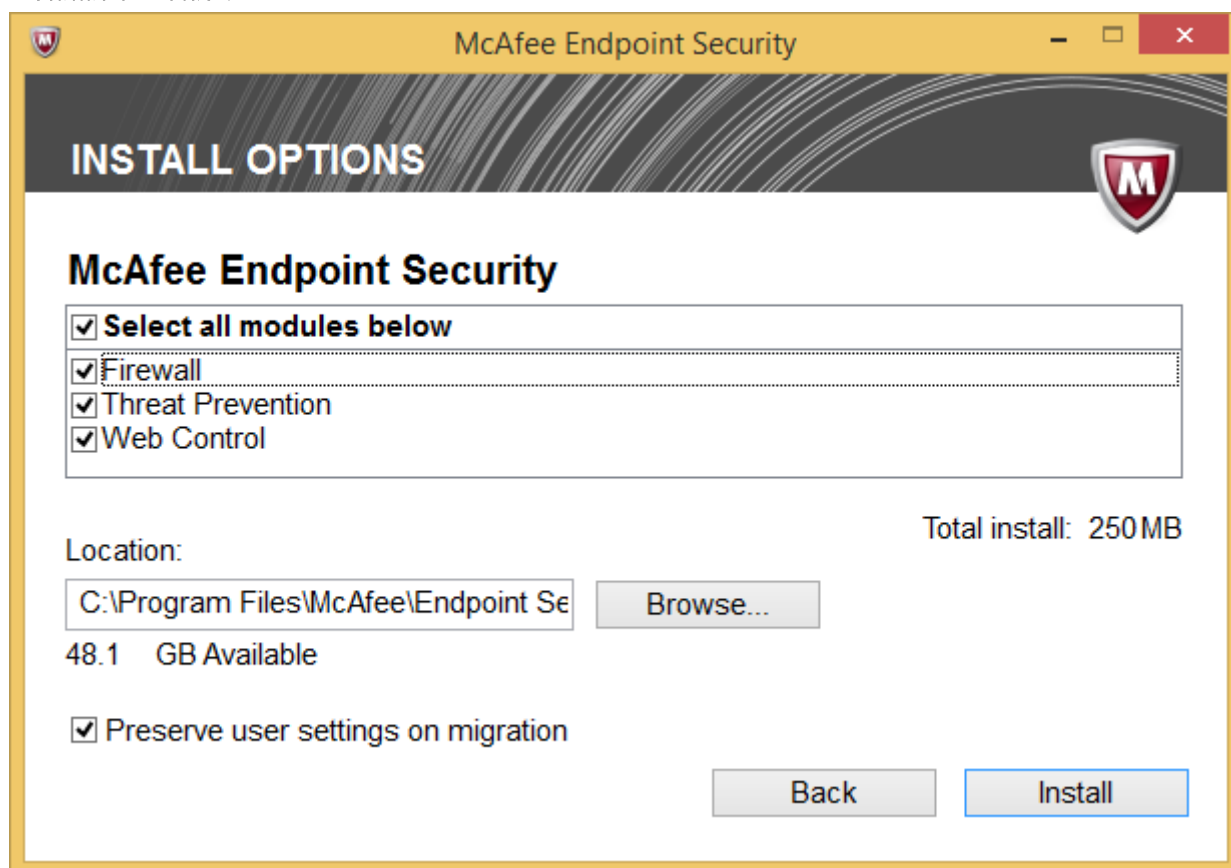
Preparing server and clients for deployment

For the local installation, no preparation of clients or server is necessary.

Deploying the software

We used the local installation method to deploy the endpoint protection software to our client PCs and server. The installation package is downloaded from McAfee as a zip file, unzipped into a folder, and made available on target computers by means of a shared folder or flash drive. There are a number of files and zipped folders in the installer directory, but the administrator only needs to execute setupEP.exe.

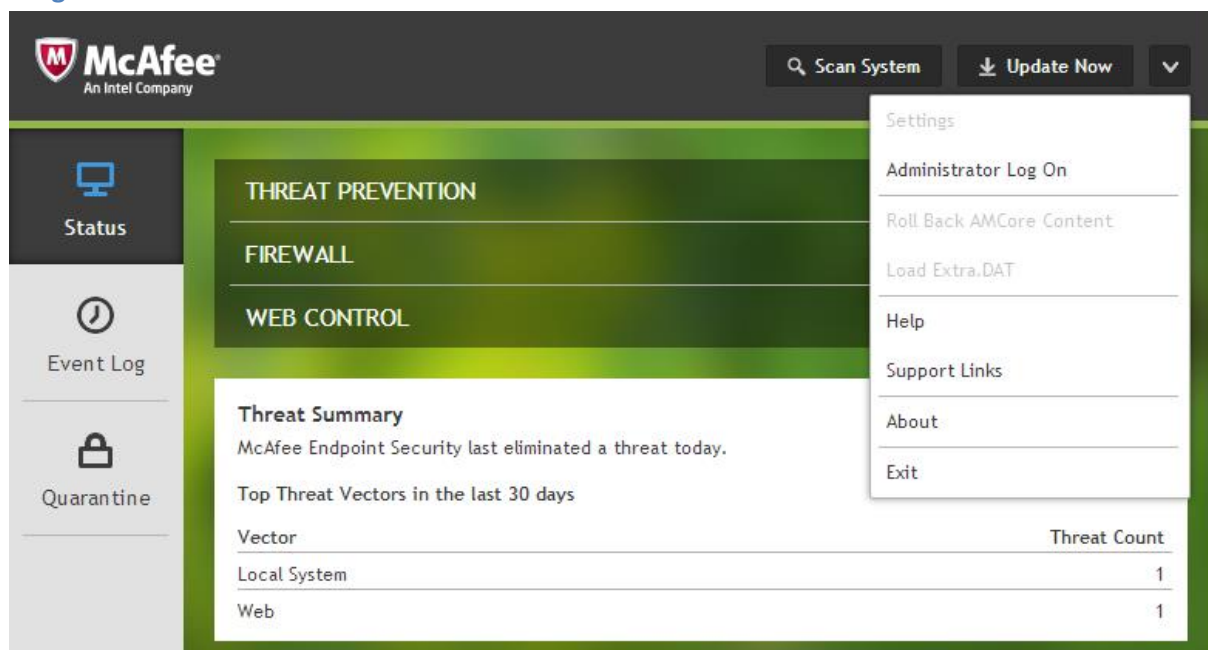
The first stage in the setup wizard involves accepting the licence agreement, and selecting a language. The admin can then choose which components to select and the location of the installation folder:



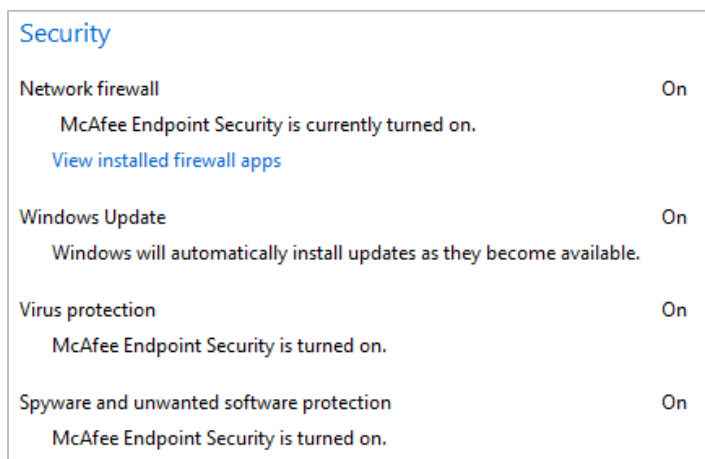
Clicking on Install then starts the installation process, which is completed a few minutes later without any further input being required.

We found the local installation of McAfee Endpoint Security to be an exceptionally simple process, and absolutely ideal for non-expert administrators in small businesses. Professionals will appreciate the choice of components and installation folder, however.

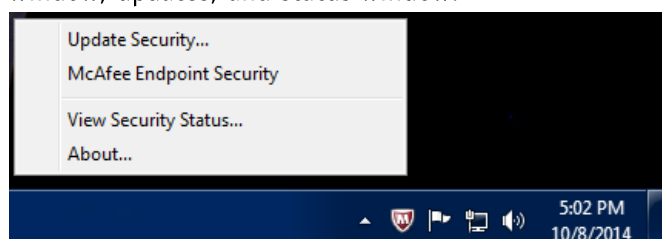
Program interface



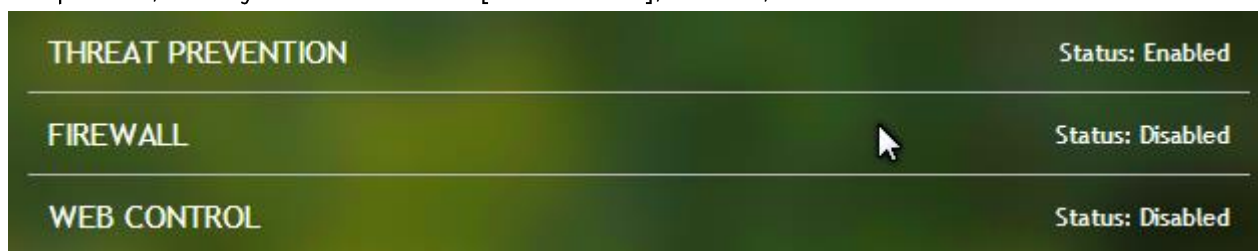
The Endpoint Security program interface can be regarded as identical for both client and server systems. There are however a number of configuration options, such as the choice of components to install. Experienced administrators may decide to take advantage of this, and configure the software differently for their server(s) than for clients. A possible scenario would be to install just the Threat Prevention (anti-malware) component on a server, and use Windows Server’s built-in firewall. Assuming the admin has chosen to install all the protection components, McAfee Endpoint Security registers with Windows Action Center as antivirus, antispyware and firewall. Windows Defender is disabled under both Windows 7 and Windows 8.



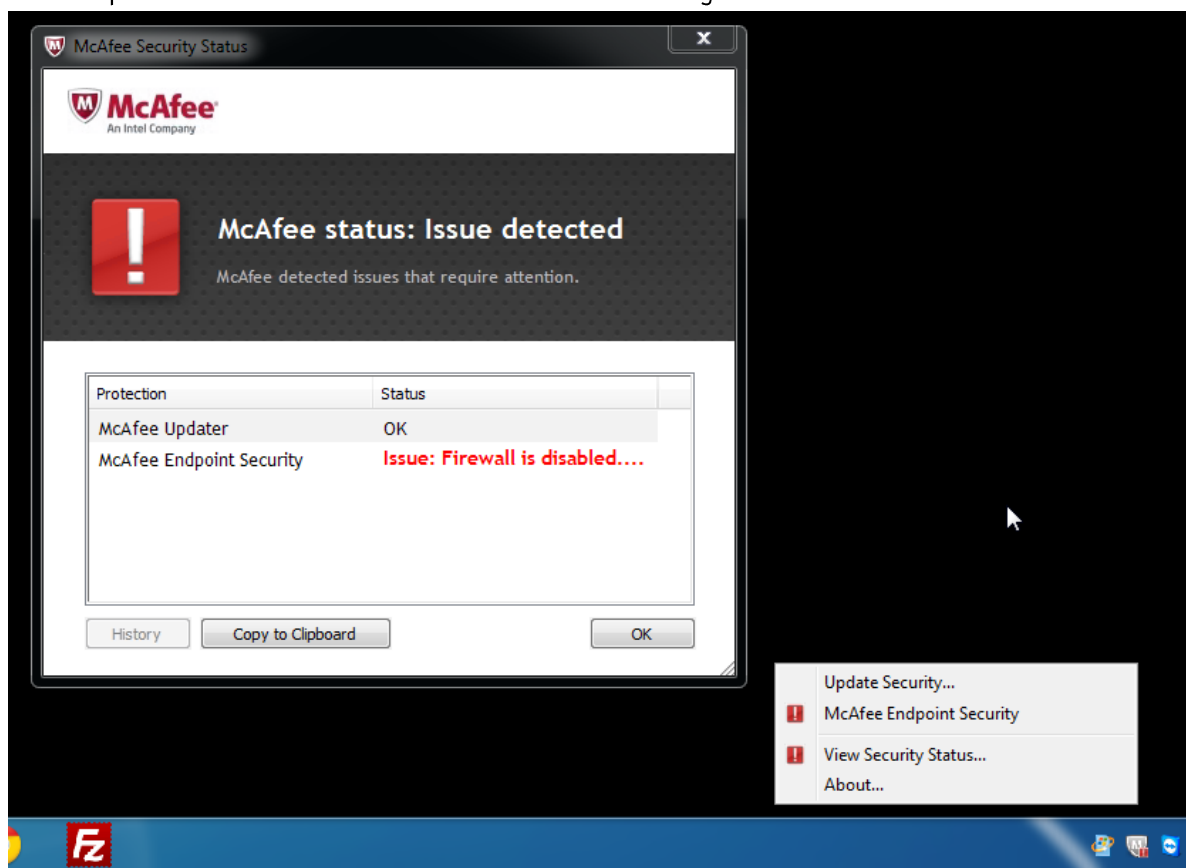
Endpoint Security installs a Windows System Tray icon, which can be used to access the main window, updates, and status window:



The status page of the client software shows the individual status of the three main protection components, namely Threat Protection [anti-malware], Firewall, and Web Control:



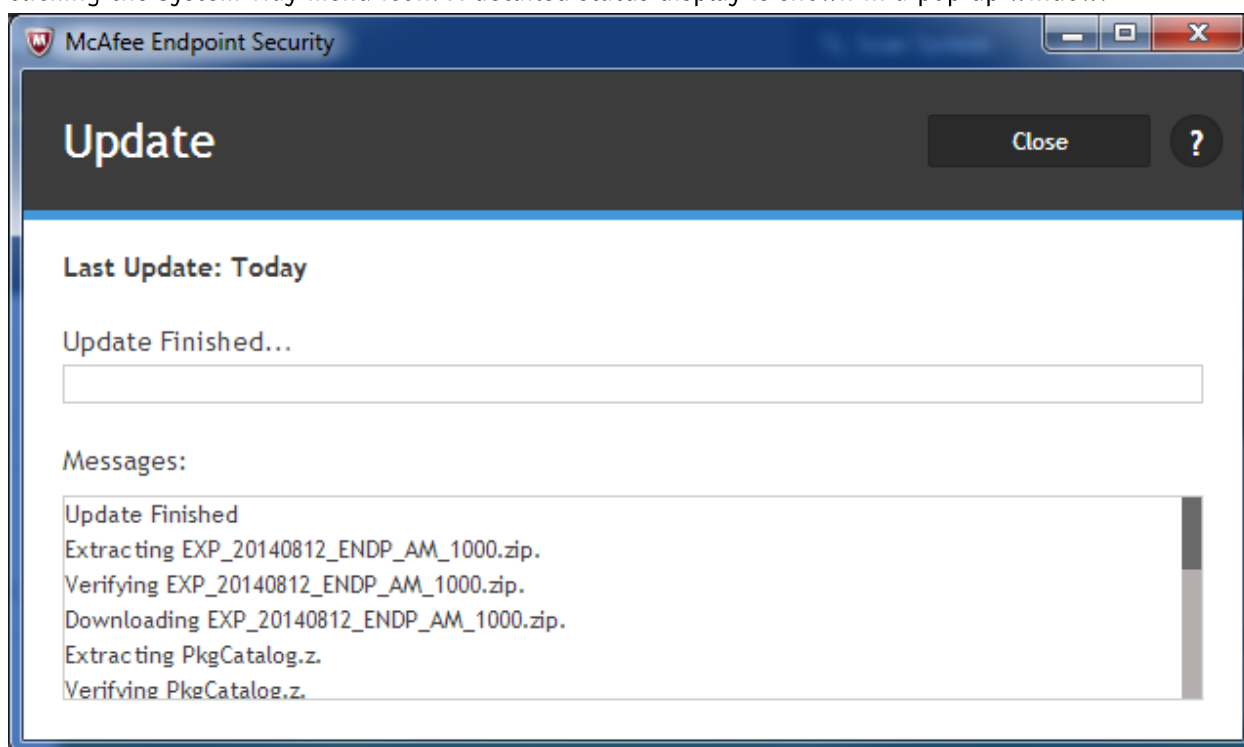
In the screenshot above, the Firewall and Web Control components are shown as disabled. McAfee also provides other alerts: the System Tray icon changes, its context menu shows alert symbols, and the independent Status window also shows a clear warning:



To reactivate a disabled component, the administrator just has to click on the component’s name in the main program window, and this will open the relevant configuration page in the settings.

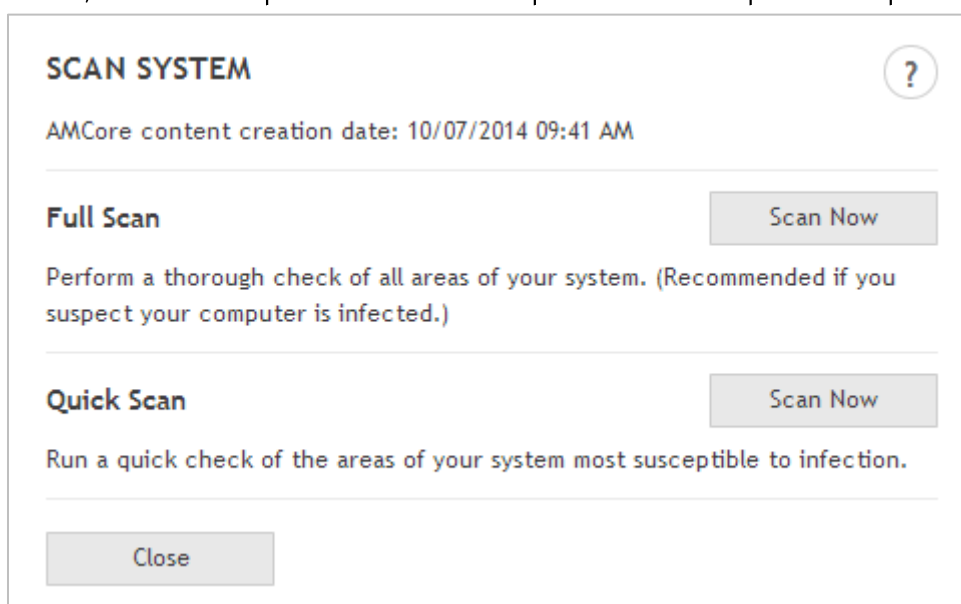
We found the program window to be very clean and simple, with a familiar layout. The status display is clear, although alerts are not very prominent in our view, and we would suggest e.g. a change of colour to make it more obvious. However, links from the component names to the relevant settings are very convenient. We found the overview of recent threats in the lower half of the window to be simple and convenient. Updates and Scans are easy to access from the prominent buttons at the top of the window, whilst logs and quarantine are also easy to find from the big buttons on the left. All other features can be found in the single drop-down menu at the top.

Manual updates can be run from both the Update Now button at the top of the window and by right clicking the System Tray menu icon. A detailed status display is shown in a pop-up window:



McAfee inform us that updates will run every four hours by default, and further update tasks can be created/modified in the Advanced Tasks section of the settings.

Scans can be run either by right clicking a drive, file or folder, or by clicking the Scan System button, also at the top of the window. This provides full and quick scan options:



Scheduled scans can be configured and run from the Tasks page in the Advanced section of the options:

Tasks				
Run Now				
Name	Feature	Schedule	Status	Last Run
Quick Scan	Threat Prevention	Daily (disabled)	Never Run	
Full Scan	Threat Prevention	Daily (disabled)	Never Run	
Default Update T...	Common	Daily	Stopped	10/07/2014 04:33 ...

McAfee allow administrators to prevent unauthorised access by means of password protection, which is configured in the settings. The possible options are: Full access; Standard access (user can run scans and updates but not change settings); Lock client interface (user cannot access interface at all without admin password). There is an option to password-protect deinstallation of the product:

Options

Tasks

Threat Prevention

Firewall

Web Control

OPTIONS ?

Client Interface Mode

Full access

Standard access

Set Administrator password:

Password:

Confirm password:

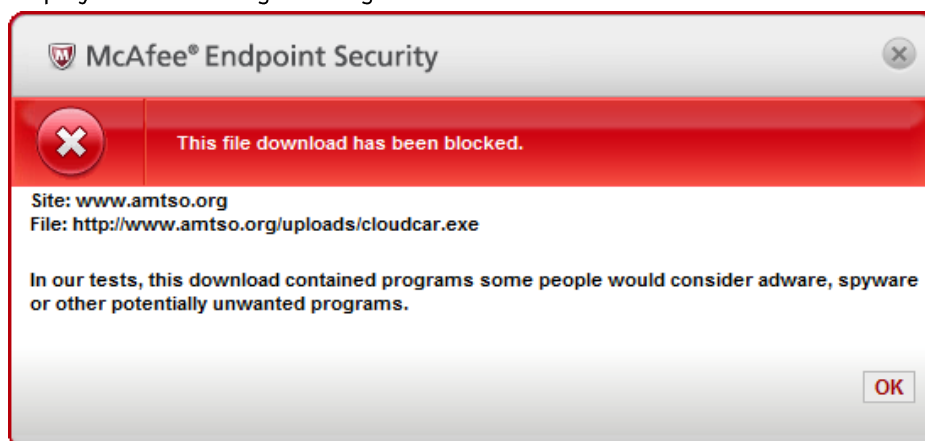
Lock client interface

Uninstallation

Require password to uninstall the client

We found the access control in McAfee Endpoint Protection to be very simple but effective, ideal for a small business.

If an attempt is made to download an AMTISO malware test file, McAfee blocks the download and displays the following warning:

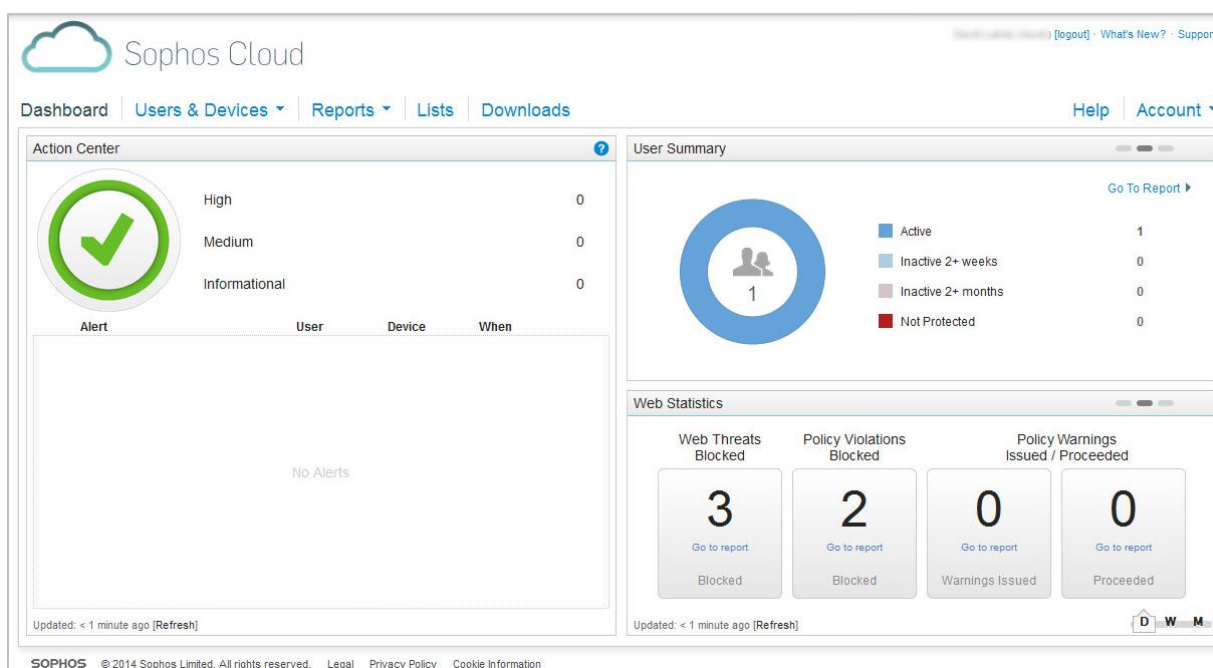


We feel the alert makes very clear to the user what has happened, and does not provide any means of letting the malware run. We consider this ideal.

Summary

We feel the Self-Managed option of McAfee Endpoint Security is very appropriate for a small office. The functionality available from the program window is ideally suited to the situation, and the interface will be clear and familiar to anyone who has used a modern consumer antivirus suite. Installation is remarkably simple but still provides suitable options. The help service provided by the program itself is clear and easily accessible. Overall, we feel the program does a remarkable job of providing the functionality a small office needs, with a clear and simple interface that will make life simple for non-expert administrators.

Sophos Endpoint Security and Control with Sophos Cloud



Introduction

Sophos specialise in making security software for business users, and produce a wide range of products for companies large and small. For our review, we used the Sophos Cloud Console to manage Sophos Endpoint Security and Control; this combination is ideally suited to our test scenario, a small business of 20 PCs and a File Server.

Software version reviewed

Sophos Cloud console, as at 24th September 2014
 Sophos Endpoint Security and Control, version 10.3 Cloud

Supported operating systems

Windows client systems: XP Pro (supported until September 2015), Vista, 7, 8, 8.1

Windows Server systems: 2003 and 2003 R2, 2008 (all 32 and 64-bit); 2008 R2, 2012, 2012 R2 (all 64-bit only).

Non-Windows platforms: Mac OS X 10.7, 10.8, 10.9; Apple iOS 7 and higher for iPhone and iPad; Google Android 4.0 and higher.

Additional features

Live Protection; HIPS; Web Security; Device Control; Web Control (Filtering); Active Directory Sync; Mobil device management (optional)

Documentation

Sophos provide a 52-page manual for the Cloud console, which explains the features of the console and how to use them. It is very accessible, thanks to bookmarks and a clickable contents page, and explains each feature clearly, albeit without illustrations. There is also an online help service, which appears to have identical content to the manual, but in a format similar to a Windows Help file.

We found the documentation to be sufficiently clear, accessible and comprehensive. However, we feel it is a great shame that there are no screenshots provided, as these would make it much quicker and easier for users to orient themselves and relate the instructions to the console itself.

Preparing server and clients for deployment

The only preparation we made on the client PCs and server was to enable Network Discovery and File Sharing.

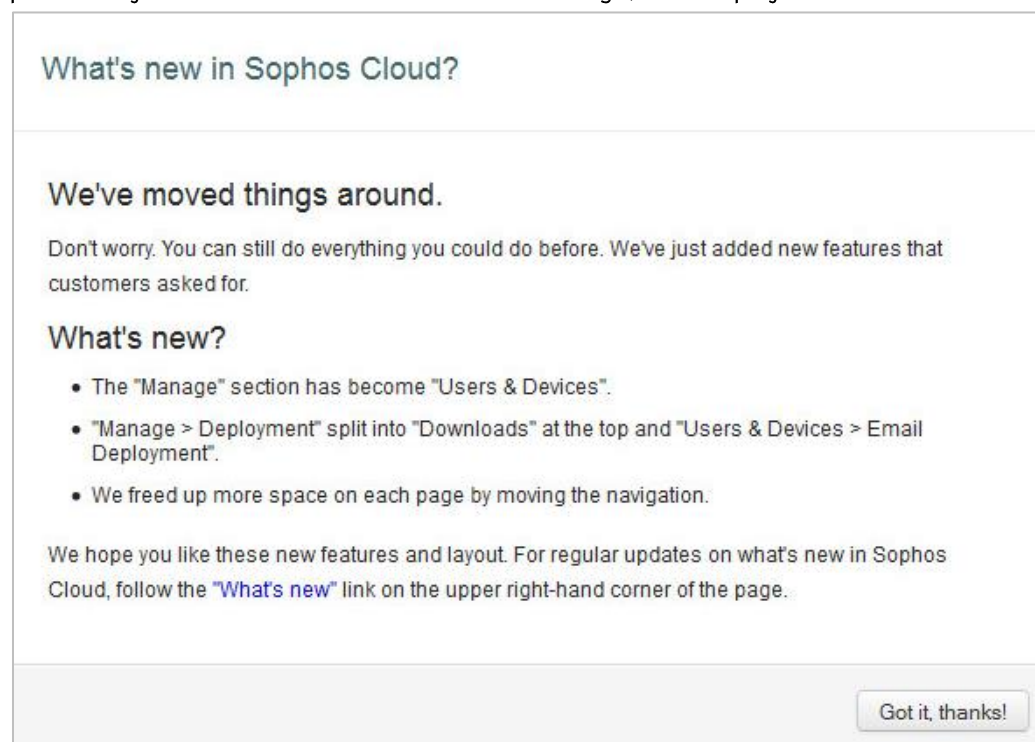
Deploying the software

The console is web-based and so requires no installation. The admin simply browses to the URL and enters the user name and password. Deploying the client software essentially involves running the installer file locally on each computer to be protected. This can be done by logging on to the console and downloading the installer on each computer; emailing a link to users with a request to install the software themselves; or downloading the installer and saving it in a shared folder on the server, which can then be accessed from each client PC. Running the installer requires minimum intervention from the admin. Once the installer has been double-clicked to execute it, there is only one option, namely whether to remove existing security software or not. The installer then proceeds by itself.

We would argue that the deployment process for Sophos Cloud could not be any simpler than it is. The installer is easily found in the console under the Downloads menu and can be run by anyone who could install iTunes. This makes it ideal for a non-expert administrator to install.

Management Console

When we first logged in to the console, a message box with details of the new console layout, presumably for users accustomed to an older design, was displayed:



What's new in Sophos Cloud?

We've moved things around.

Don't worry. You can still do everything you could do before. We've just added new features that customers asked for.

What's new?

- The "Manage" section has become "Users & Devices".
- "Manage > Deployment" split into "Downloads" at the top and "Users & Devices > Email Deployment".
- We freed up more space on each page by moving the navigation.

We hope you like these new features and layout. For regular updates on what's new in Sophos Cloud, follow the ["What's new"](#) link on the upper right-hand corner of the page.

Got it, thanks!

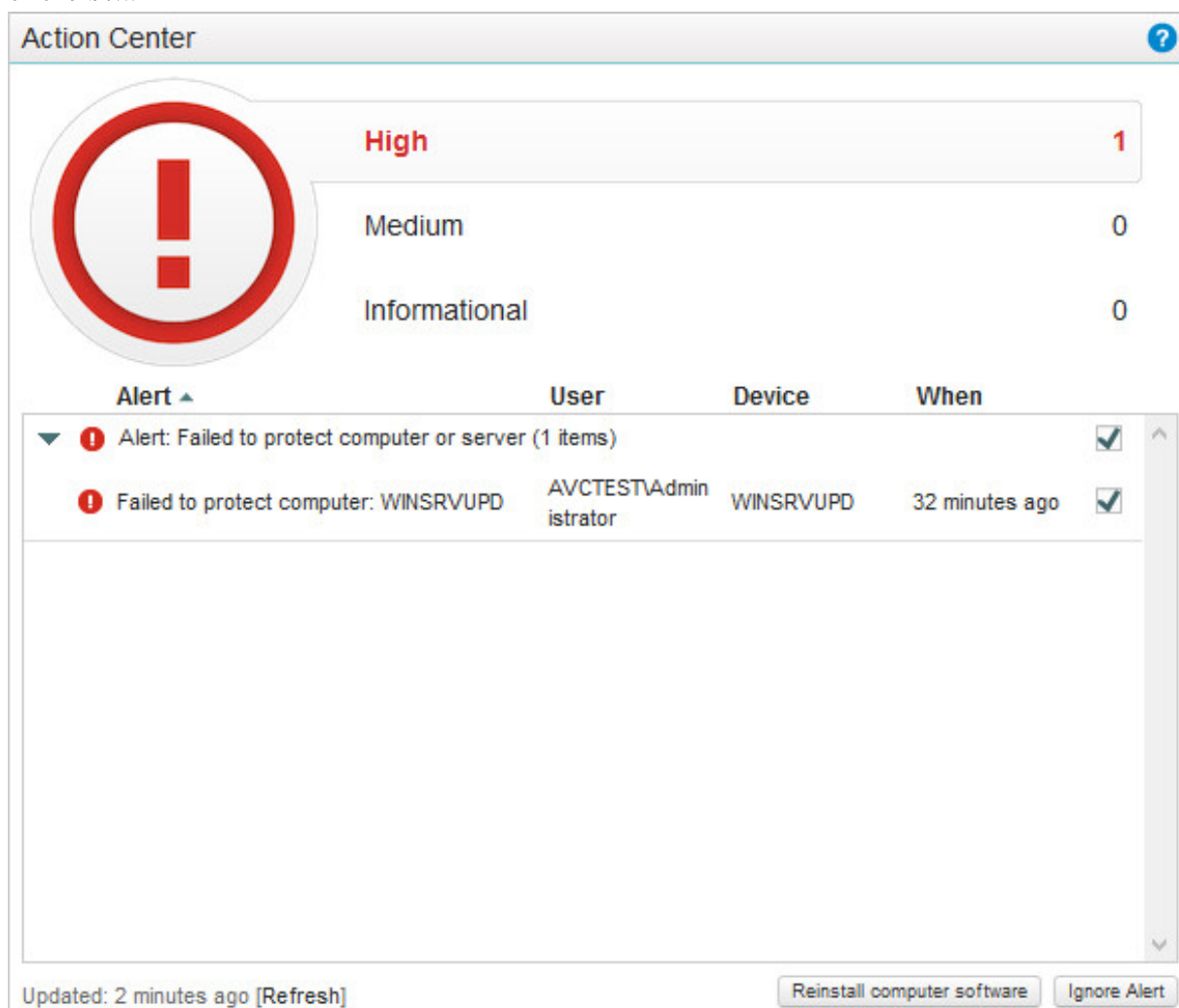
When we dismissed this, the Dashboard (console home page) was shown. This consists of one main panel on the left-hand side called Action Center, which displays alerts.

The right-hand side of the console is divided into 2 boxes, each of which shuffles through 3 possible display items, like a slideshow. The upper one shows Mobile Summary, Computer Summary, and User Summary, whilst the lower one displays Global Activity, Web Statistics and Resolved Malware Detections. The Console’s controls are completed by a menu bar at the top of the page, showing Dashboard (the home page just described), Users & Devices, Reports, Lists (for web-content filtering), Downloads, Help, and Account.

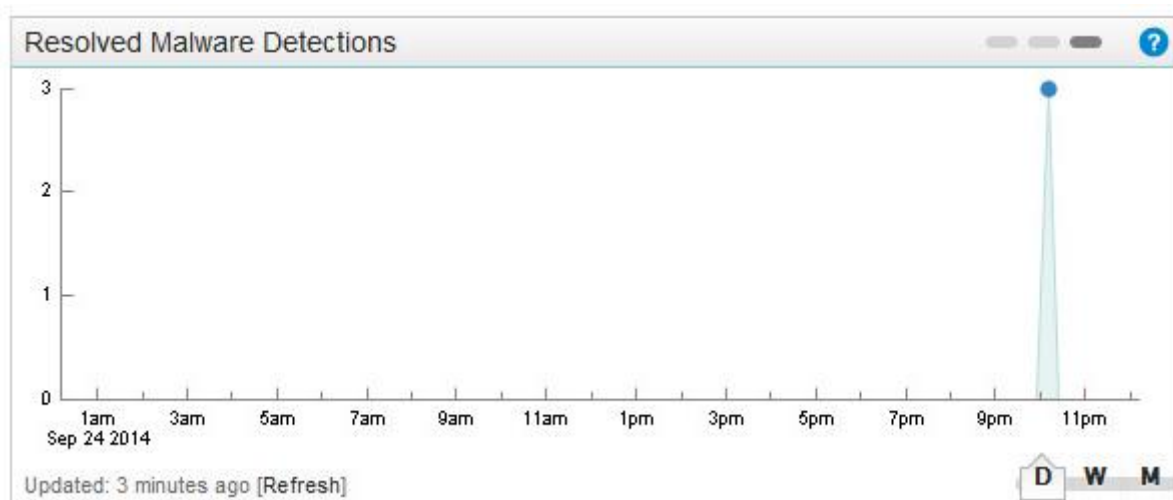
We found the information box explaining the new layout to be a sensible idea that would be helpful to existing users. The console itself has a very clean and uncluttered appearance, which does not overwhelm the admin with information or controls. We did however find the “slideshow” of items in the right-hand 2 boxes to be rather annoying, as we had to wait for the thing we wanted to see, only to find it wasn’t there for very long. We could not find any means of customising this, but suggest that such an ability would be an improvement. Ideally, the admin could choose how many items are displayed in each box, change the time each item is displayed, or simply turn the slideshow off altogether and display a greater number of static boxes on the page.

Monitoring the network

In the event of a problem, the Alerts panel shows clearly what is wrong, and provides a means of putting it right, in this case by displaying the “Reinstall computer software” button at the bottom of the box:



Malware detected and deleted by clients is shown in the Resolved Malware Detections box on the Dashboard, in the form of a graph showing number of detections per hour and day:



We could not find a means of displaying the program version of the client software in the console. Licensing information can be seen by clicking the Account menu and then Administration.

The Action Center makes important alerts very visible, and providing suitable controls to rectify any problem shown is extremely practical. The Malware Detections box provides a useful at-a-glance view of malware detection history.

Managing the network

A manual update can be run on an individual computer by clicking the Users and Devices menu, Devices, and then the name of the computer concerned. Scheduled Scans can be set in the console, by editing the policy applied to each PC, as shown below. This could also be used to run manual scans on individual computers.

Scanning options for malware and risky file types.

Enable real-time scanning

Enabled scheduled scan at 21:00 on Mon Tue Wed Thu Fri Sat Sun All Weekdays

Scan inside archive files (with extensions .zip, .cab, etc.)

[Scanning Exemptions](#) ▼

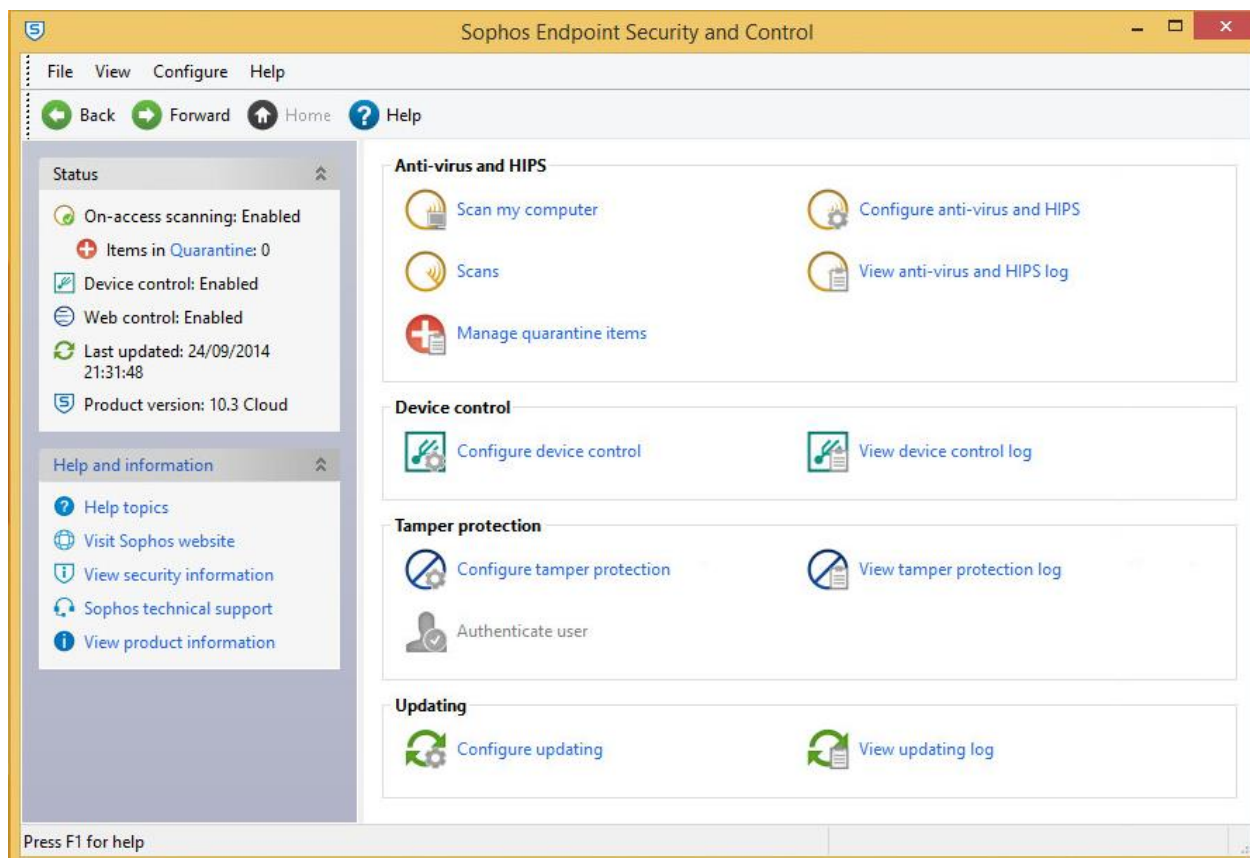
We note that updates and scans can also be run locally on any PC by using the client software, an entirely feasible option in a small office.

We found the means of scheduling a scan to be particularly simple and convenient.

Client antivirus software

Sophos Endpoint Security and Control installs a Windows System Tray icon, which can be used to run updates and open the main program window. The software also registers with Windows Action Center as antivirus and antispyware. Windows Firewall is not disabled (as Sophos does not install a firewall of its own). Windows Defender is disabled under Windows 8, but not under Windows 7.

Protection status is shown, somewhat discretely, in the top left-hand corner of the window, as a list of protection components, each one as marked as Enabled or Disabled. An update can be run by right-clicking Sophos' System Tray icon and then clicking Update. The home page of the program window provides buttons for complete and custom/scheduled scans.

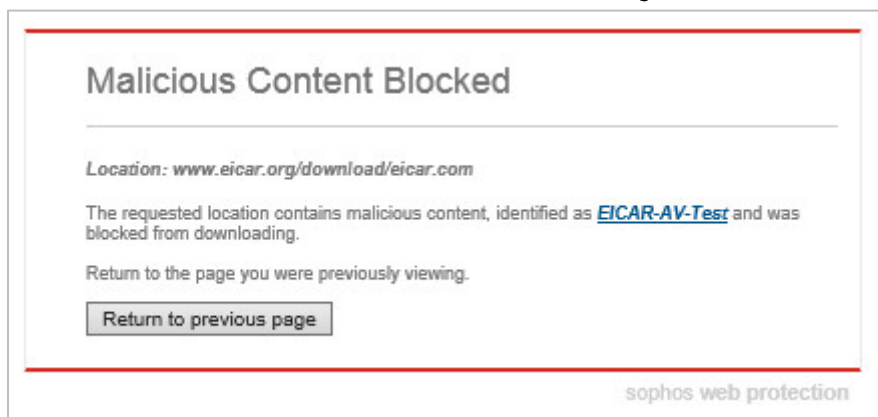


By default, Sophos’ Tamper Protection feature prevents even administrators from disabling real-time protection from the client window. If Tamper Protection is disabled from the console, the protection can be disabled by administrators only, not by standard users. If the admin needs to disable RTP temporarily, e.g. to install a particular program, he or she can quickly log on to the console, switch off Tamper Protection, disable RTP locally, and then re-enable both when the program has been installed.

When real-time protection is disabled, Windows 7 shows a System Tray pop-up warning, while Windows 8 shows one of its alert boxes in the top right-hand corner of the screen:



When the EICAR test file is downloaded, the following alert is shown in the browser:



The client software allows users to run updates and scans, but not change any protection settings, which we find ideal. Relative to the very modern and clear design of the console, we found the main program window somewhat old-fashioned (graphically reminiscent of Windows XP's Explorer). We suggest it could be given a more modern and cleaner design, and made a little more friendly to non-expert administrators. Ideal additions would be an update button and a more visible status display with a Fix-All button to re-enable protection in the event of a component being disabled. The Tamper Protection feature strikes us as an excellent safeguard against unauthorised changes to the configuration, which nonetheless can be temporarily disabled by the admin if necessary.

Server antivirus software

Currently, this is identical to the client software. However, Sophos inform us that they are going to release an update, planned for mid-November, in which the server software will differ from the client. The same installer will be used for both types of computer, and this will automatically recognise whether it is being installed on a client or server operating system, and apply the appropriate policy.

Summary

Sophos Cloud is tailor-made for small businesses without full-time IT professionals on the staff. The software could easily be deployed by a non-expert administrator, as the web-based console does not require any installation or configuration, and installing the endpoint protection software literally only requires a couple of clicks. The console is simply and clearly laid out, but provides a number of features. We have just a couple of suggestions for improvement: some screenshots for the manual, a facelift for the client software window, and some ability to customise the console.

Symantec Endpoint Protection Small Business Edition

The screenshot shows the Symantec Endpoint Protection Small Business Edition web console. The interface is dark-themed with a navigation bar at the top containing 'Home', 'Computers', 'Policies', 'Users', 'Alerts', 'Reports', 'Settings', 'Subscriptions', and 'Support'. The main content area is divided into several sections:

- Computer Health:** Shows a 100% health status with three indicators (green checkmark, yellow warning, red X) and counts: 1 computer, 0 warnings, 0 errors. A message states 'There are no computers at risk.'
- Quick Tasks:** Includes links for 'Add Computers', 'Add Users', 'View Invitation History', and 'Buy Additional Subscriptions'.
- Endpoint Protection Summary:** Provides a summary over the last 7 days:

Total Computers:	1	Quarantined Items:	0
Viruses:	0	Unresolved Security Risks:	0
Blocked USB Devices:	0	IPS Blocked:	0
		Other Risks:	0
- Virus and Risk Activity Summary:** States 'Last updated: N/A' and 'There is no data available over the last 7 days.'
- Services:** Shows a table for subscriptions:

Subscription	Time Remaining
Endpoint Protection 50 licenses (1 in use)	30 days

Introduction

Symantec produce an enormous selection of software products for businesses of all sizes. For this review, we have looked at Symantec Endpoint Protection Small Business Edition, which uses a cloud-based console to manage endpoint protection software for clients and file servers.

Supported Operating Systems

Internet Explorer, Firefox and Chrome browsers are supported for the cloud console. The protection software runs on Windows XP, Vista, 7, 8, 8.1, and Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2, all with 32 and 64-bit architecture.

Non-Windows platforms: Mac OS X 10.6.8, 10.7, 10.8; Mac OS X Server 10.6.8, 10.7, 10.8, 10.9

Additional features

Client firewall;

Documentation

Symantec produce two manuals for the product, a 108-page Administrator Guide and an 80-page Getting Started Guide. Both cover the essentials of deploying the endpoint protection to the clients. There is also a searchable online knowledge base.

Both manuals are clearly organised, well written and easily accessible through bookmarks and a hyperlinked contents page. The Administrator Guide is not much longer than the Getting Started Guide, and the same information on deployment is found in both. This left us feeling rather confused as to which manual to use, as we did not feel it was clear what the differences between

the two were. The online knowledge base quickly found helpful answers to two fairly standard queries. As with both the manuals, there are no screenshots at all, which we feel is a great pity.

Preparing server and clients for deployment

We enabled File Sharing and Network Discovery on our client PCs; no other preparation was necessary.

Deploying the software

The console is cloud-based and so does not need any installation. The admin simply enters the URL in a browser and logs on.

There are a number of ways to deploy the endpoint protection software to the clients. An Active-Directory-ready installation package can be created for deployment by Group Policy, a method suited to experienced admins and larger networks. Alternatively, the administrator can email users a link to the software for them to install themselves, if they have administrator rights on their own computers. Other possibilities include downloading the software from the console and installing it locally on each PC, or saving the installer file to a shared folder on the server, and accessing this from each client. We used the latter method in our test.

We feel the variety of installation methods makes the product easy to install on both small and large networks. For smaller businesses and/or less experienced administrators, running the installer locally on each machine is ideal, as it is a simple process which does not require specialist knowledge.

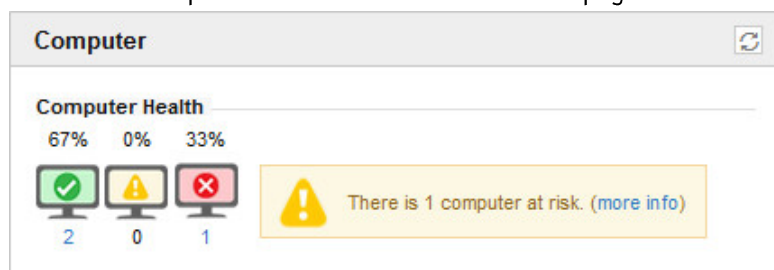
Management Console

The home page of the management console displays a number of panels displaying data and tasks, including Computer Health (percentage of clients in normal/warning/problem status), Services (subscription information), Quick Tasks, and Virus & Risk Activity Summary. The page can be customised, by dragging & dropping and displaying or hiding individual panels. There is a row of tabs along the top of the console which display the pages Computers, Policies, Users, Alerts, Reports, Settings, Subscriptions, and Support.

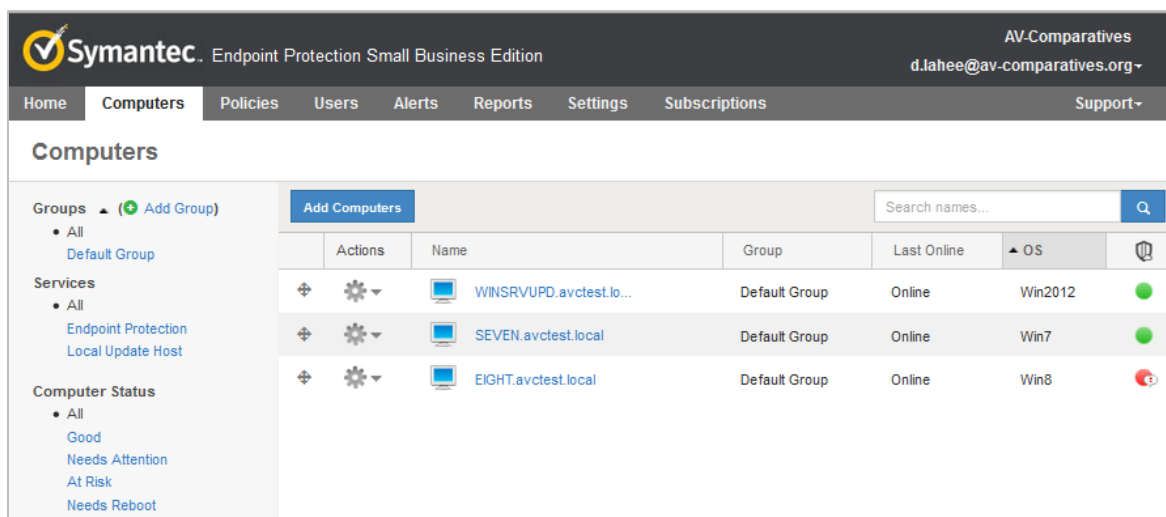
We feel the console has been extremely well designed, is easy to navigate and makes all essential information and tasks easily accessible. The ability to customise the home page particularly impressed us. The admin can very quickly and easily add or remove panels, and change their position on the page, to ensure that the items he/she wants to find quickly can be seen at a glance. A single row of tabs along the top of the console makes navigating between pages very straightforward.

Monitoring the network

If any of the client PCs requires attention or is displaying an alert, this can be seen at a glance in the in the Computer Health Panel on the Home page:

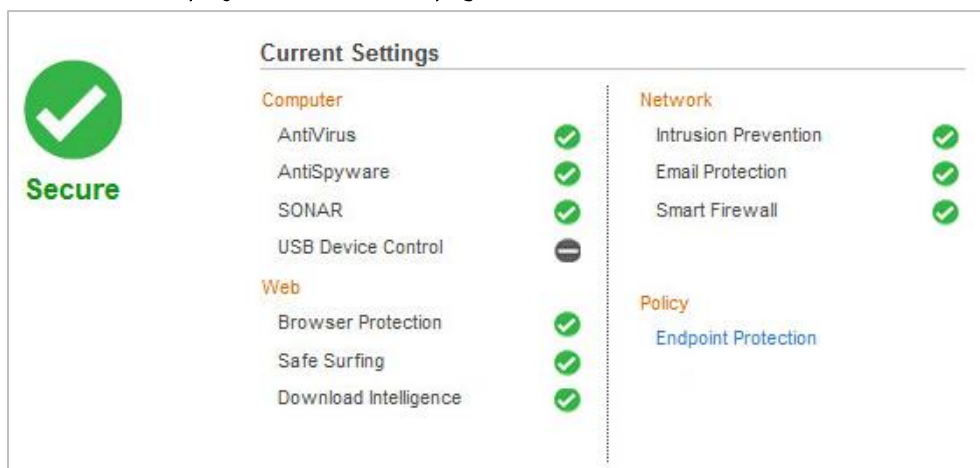


The Computers page of the console displays all managed machines along with their online and protection status:

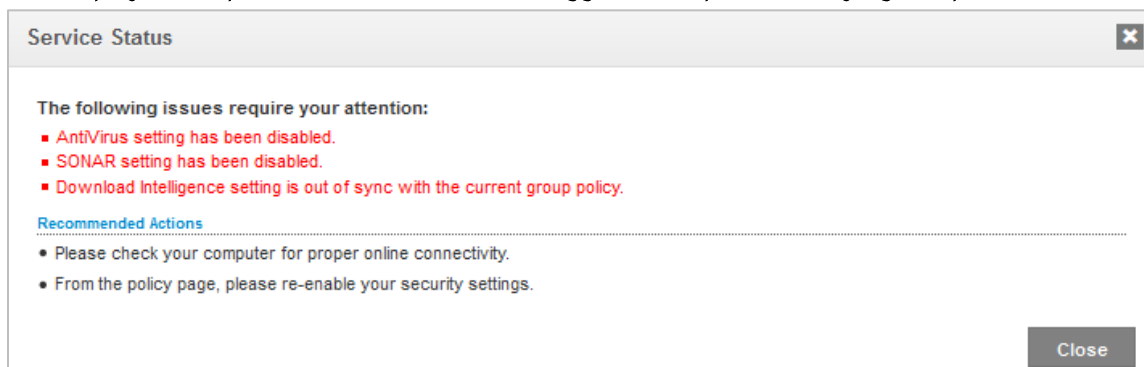


The Computer Status menu on the left provides a filter that can display only those machines deemed At Risk, Needs Attention, or Needs Reboot. This can be used manually by the administrator, but is also used automatically by the console itself, showing only computers at risk, if the admin clicks the “more info” in the Computer Health panel.

The Actions menu on the Computers page allows scans and updates to be run. Clicking on the name of an individual computer shows a very detailed status page, which is more or less identical to the information displayed on the home page of the client software:



The same page also shows the version of the client software and the operating system, along with a summary of risks (firewall and malware detections etc.) encountered in the last week. In the event that a computer is at risk, a link entitled “more info” will be displayed on the client page. Clicking this displays an explanation of the risk, and suggested steps for rectifying the problem:



Malware detections which have been safely dealt with by the client software are not shown in the console. A licence summary is shown on the home page, while more detailed information can be displayed from the Subscriptions menu:

Symantec Endpoint Protection Small Business Edition

Total Licenses: **50 licenses**
Usage: **3 licenses**

[Download On-Premise Manager](#)

Subscription Details

Type	Serial Number	Quantity	Start Date	End Date
Trial	TRIAL-1338204968	50 licenses	Saturday, October 04, 2014	Monday, November 03, 2014

We regard the Computer Health panel on the Home page is a remarkably effective but simple means of showing the administrator whether all is well. The “more info” link provides instant access to a more detailed view of the computers affected on the Computers page, and this in turn enables details of individual computers to be shown with a single click. Our only suggestion for improvement would be to add a “Fix” button to the information box that shows exact details of the issues and suggested solutions. Otherwise we feel the console is unbeatable for simplicity and effectiveness of monitoring a small business network.

Managing the network

Updates, along with both quick and full scans, can be performed on an individual computer by mousing over its Actions symbol on the Computers page:

The screenshot shows a table of computers with columns for Actions, Name, Group, Last Online, OS, and a status icon. A context menu is open over the computer 'SEVEN.avctest.local', showing the following options:

- Endpoint Protection
 - Quick Scan
 - Full Scan
 - Check Virus Definition

Alternatively, clicking “Perform Group Actions” in the menu panel on the left-hand side of the console allows an entire group to be scanned or updated at once:

Group Action [X]

What type of group action would you like to perform?

Search names... [Q] [X]

Computer Group [Select All | None](#)

Default Group

Note: Only computer groups with one or more associated computers will show up in this list.

Endpoint Protection

Group Scan

Quick Scan - Scan commonly infected areas

Full Scan - Scan your entire computer

Note: A full system scan can take up to a few hours to complete

Live Update

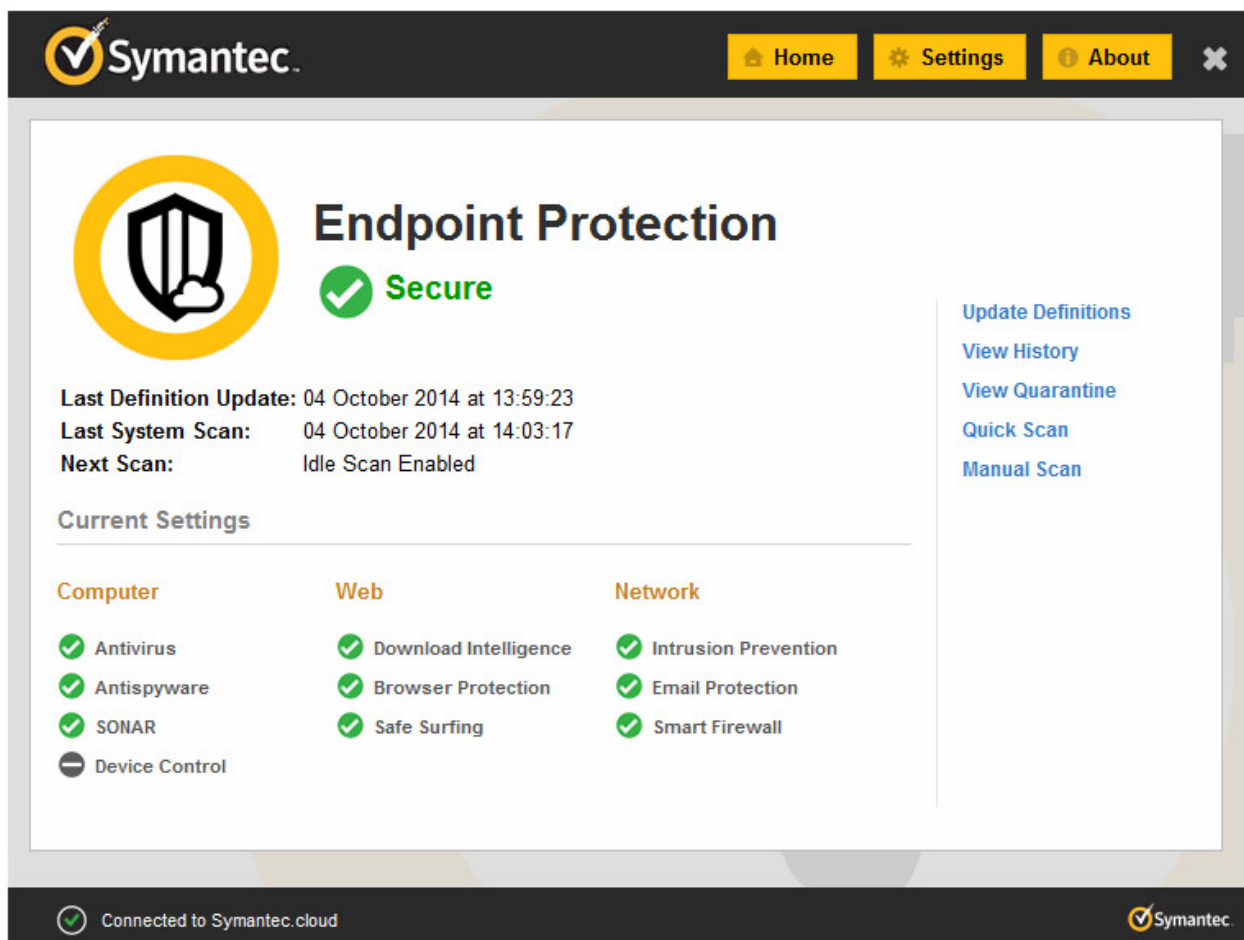
Run LiveUpdate - Check for the latest virus definition

Perform Action **Cancel**

Running scans and updates is very simple on individual computers; it is also very easy for groups, provided one has found the link in the menu panel. We feel this would be more noticeable if it were placed e.g. next to the Add Computers button at the top of the Computers panel.

Client antivirus software

Symantec Endpoint Protection registers with Windows Action Center as firewall, antivirus and antispyware. Windows Defender is disabled under Windows 7 and Windows 8. There is a System Tray icon, which can be used to run scans and updates. Updates, quick scans and custom scans can be run from the main program window. There is an obvious status display in the form of text and icon on the home page:



By default, real-time protection cannot be disabled from the client software by the admin or any other user. However, the admin can create and apply a new policy to a computer or group, which either disables the protection or allows the user to do so:



This would be useful if the admin needed to install a program whose setup wizard requires antivirus to be temporarily disabled. The program window shows an alert when the protection is disabled; it can be reactivated by clicking either FIX or Enable Antivirus in the menu panel on the right:



Endpoint Protection
✘ At Risk

[FIX]
[Update Definitions](#)
[View History](#)
[View Quarantine](#)
[Quick Scan](#)
[Manual Scan](#)
[Enable Antivirus](#)

Last Definition Update: Sunday, October 05, 2014 at 3:45:52 PM
Last System Scan: Sunday, October 05, 2014 at 4:30:44 AM
Next Scan: -

Current Settings

Computer	Web	Network
✘ Antivirus	✘ Download Intelligence	✓ Intrusion Prevention
✓ Antispyware	✓ Browser Protection	✓ Email Protection
✘ SONAR	✓ Safe Surfing	✓ Smart Firewall
☐ Device Control		

When the EICAR test file is downloaded, the following alert is shown:



The client antivirus software should appear familiar to anyone who has used typical consumer antivirus software. It allows the user to run updates and scans easily, but makes it impossible to disable protection components. This strikes us as a very sensible default setting.

Server antivirus software

This could be regarded as the same as the client software, but configured slightly differently. The firewall and email protection components are not installed, and the “Update Definitions” link is not shown.

Summary

We would describe Symantec Endpoint Protection Small Business Edition as an outstanding product that would make life very easy for any small-business administrator. It has been extremely well designed at every level. The console is cloud-based and so requires no installation, while there is a variety of client-software deployment methods, including a very simple local installation process ideal for smaller networks and inexperienced administrators. We particularly liked the fact that the Home page of the console can be so easily customised, and that alerts provide convenient links to pages showing more details and suggested solutions. The client software has a familiar design and sensible default settings. Our only significant suggestion for improvement is that the well-written manuals should be illustrated with screenshots.

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G DATA	Ikarus	Kaspersky Lab	McAfee	Sophos	Symantec
Recommended product for:										
up to 5 Clients, Server	Avira Endpoint Security	Small office Security (Cloud) by Bitdefender	ESET Endpoint Security	F-Secure Business Suite	G DATA Small Business Security	IKARUS anti.virus	Kaspersky Small Office Security	McAfee Small Business Security	Sophos Endpoint Protection - Business	Symantec Endpoint Protection Small Business Edition
up to 25 Clients and 1 Fileserver	Avira Small Business Security Suite	Small office Security (Cloud) by Bitdefender + Bitdefender Security for Exchange	ESET Small Business Security Pack 20		G DATA Endpoint Protection Business	IKARUS security.manager	Kaspersky Endpoint Security for Business + Kaspersky Security for Mail Server		McAfee Endpoint Protection Advanced	
up to 25 Clients and Fileserver and Messaging Server			ESET Business Solutions		G DATA Endpoint Protection Business + MailSecurity + ClientBackup					
more than 25 Clients, more than 1 Fileserver, more than 1 Messaging server										
Features Management Server										
What is the maximum number of clients overall?	2 000	unlimited	unlimited	unlimited	unlimited	unlimited	unlimited	300 000	25 000	800 000
What is the maximum number of clients that can be managed from a single management server under the following conditions: All necessary components (database, repositories, update mechanisms, reporting, etc.) are installed on this server and the Clients communicate with the server either continuously or at least once per hour	2 000	unlimited	depends on hardware of the server and the database used	20 000	1 000	unlimited	25 000	unlimited	25 000	50 000
Required <u>minimum</u> hardware (CPU/RAM/free disk space)	1GHz, 1GB RAM, 5GB disk space	The server is hosted in-the-cloud.	1GHz, 512MB RAM, 1GB disk space	2 GHz, 1GB RAM, 6GB disk space	2GHz, 2GB RAM, 3GB disk space	2GHz, 1GB RAM, 500MB disk space	1GHz, 512MB RAM, 1GB disk space	2.66GHz, 8GB RAM, 20GB disk space	1GHz, 512MB RAM, 500 MB disk space	2 GHz, 4GB RAM, 100GB disk space
Does the product provide a mechanism to limit the data transferred over WAN Links when updating clients in remote locations?			*	*	*		*	*	*	*
By designating one client as local source for definition updates (Super Agent, Group Update Provider)	*	*	*	*	*	*	*	*	*	*
Which options does the product provide to ensure that only authorized administrators can administer the product?	Login/Users + ACL	Role based user models enforced through passwords	Password protection, complex password option, Windows domain authentication (role based management), encrypted communication	Password-based user authentication in Policy Manager Console	Role based user model enforced through passwords / AD Login/Windows based Login / password-protected client / encrypted communication between server and client and server and administrative console	Password protection of the server	Authentication username and password supporting RBAC, password-protected client, system tray icon hide	Authentication as well as cert based authentication of administrators into ePO, audit logs to log who has made policy changes	Password protection, encrypted communication, role-based administration	Passwords, RSA SecureID, Active Directory Authentication
Log out administrator if idle for a specified time		*		*	*		*	*	*	*
Master-Slave-Server										
Multiple AV Servers			*		*		*	*		*
Master server controls slave server in different offices			*		*		*	*		*
Slave server for distributing updates	*		*	*	*	*	*	*		*
Notes		Management server infrastructure is hosted in-the-cloud, providing High Availability and unlimited scalability. Individual Update Servers can be installed into LAN. It is possible to install and configure more Update Servers in cascade.	Slave servers can be nested in multiple levels, each with its own credentials for access, which can be dependent on administrator's role (read-only/limited user/full privileges). Policies from upper level servers could be propagated to lower levels.		Different deployment possibilities, such as: All in one management server deployment, redundant server deployment (Main and Secondary ManagementServer), combination between management server and cascaded subnet servers (Update agent) and/or Peer-to-Peer update distribution between clients, multiple management servers based for example on their location and managed with G Data Master Administrator, or combination of the above	every workstation/server with a simple windows fileshare can be used as a "distributing update server"				

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G DATA	Ikarus	Kaspersky Lab	McAfee	Sophos	Symantec
Client Installation										
Which client deployment methods does the product support?										
Does the product include a mechanism that allows the administrator to push the software to the clients?	*	*	*	*	*	*	*	*	*	*
Can the installation of the clients be staggered over time to ensure that the network is not over utilized?	*		*	*	*		*	*	*	*
Can the administrator see the status of the deployment (i.e. Transfer, Installation in Progress, Installation complete, etc.)?		*	*	*	*	*	*	*	*	*
Does the product include a mechanism that allows the end user to download and install the software?		*	*	*	*		*	*	*	*
Can the admin send a link which allows the user to download and install the software?		*	*	*	*	*	*	*	*	*
Does to product support the creation of MSI packages for deployment with 3rd party tools and Active Directory (GPO)?			*	*			*	*		*
Does the product support the creation of single file executable (.exe) installer (i.e. for logon scripts or CD distribution)	*	*	*		*	*	*	*	*	*
Group Import & Synchronisation										
Can computers be imported from a text file?	*		*		*	*	*	*	*	
Can computers be imported from Active Directory?	*		*	*	*	*	*	*	*	*
Keeping the OU structure defined in Active Directory	*		*	*	*	*	*	*	*	*
Using other criteria to assign computers to groups	*		*	*	*	*	*	*		*
Can changes in Active Directory be synchronized?	*		*		*	*	*	*	*	*
Can the synchronisation schedule be defined?	*		*		*	*	*	*	*	*
Can computers be imported from multiple Active Directory server?				*	*		*	*		*
Can computers/users be imported from other LDAP server?			*	*		*	*			*
Can computers be imported by a GUI	*		*	*	*	*	*	*		*
Can different actions be defined based on the malware category?			*		*	*	*	*	*	*
Scan Location										
Can the administrator exclude/include files and folders from being scanned (by file extension)?	*	*	*	*	*	*	*	*	*	*
By predefined lists of extensions provided by the product	*	*	*	*			*	*	*	*
By filenames ("file.txt") regardless of folder or location	*			*	*	*	*	*	*	
By filenames, foldername & specific folder ("c:\Directory\file.txt")	*	*	*	*	*	*	*	*	*	*
Standard Windows folder (i.e. %WINDOWS%, %SYSTEM32%) regardless of the operating system language	*	*	*	*		*	*	*		*
Does the product provide preconfigured exclusions?	*	*	*	*			*	*	*	*
Microsoft Exchange										
Microsoft Exchange	*	*	*	*	*		*		*	*
Network shares										
Is scanning of network shares disabled by default?					*	*	*	*	*	
Can a user or administrator scan network shares after entering a password?			*				*	*		*
System memory / Processes										
Does the product scan processes in memory for malware?	*	*	*	*	*	*	*	*	*	*
Can the administrator define exceptions?	*	*	*	*	*	*	*	*		*
Boot sectors										
Email Messages										
Does the product scan existing email in the message stores of the following applications?										
Microsoft Outlook / Outlook Express	*	*	*	*	*	*	*		*	*
Lotus Notes	*				*				*	*

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G DATA	Ikarus	Kaspersky Lab	McAfee	Sophos	Symantec
Thunderbird	*	*	*		*		*		*	
Microsoft Windows Live Mail	*		*		*		*		*	
Microsoft Windows Mail	*	*	*		*		*		*	
Does the product scan incoming and outgoing emails and attachments in the following protocols?										
SMTP / POP3	*	*	*	*	*		*		*	*
IMAP	*		*	*	*		*		*	*
Archives										
ZIP/RAR/ARJ & archived installers	*	*	*	*	*	*	*	*	*	*
how deep at on demand (by default)	20	16	10	5	100	8	unlimited	3	10	3
On Demand Scans										
Can the administrator define when scans should take place and which Scan locations should be included / excluded?	*	*	*	*	*	*	*	*	*	*
Can the system impact vs. scan speed be defined?	*	*	*		*		*	*	*	*
On Access Scan										
Can the administrator define when a scan is triggered?	*	*	*	*	*	*	*	*	*	*
Can the administrator specify which Scan Locations (incl. Files / Directories) should be included / excluded?	*	*	*	*	*	*	*	*	*	*
Which information is logged?										
Date and time the infection was detected, the name of the infection and the original location where the infection was found (incl. file name)	*	*	*	*	*	*	*	*	*	*
The malware category (i.e. Virus, Worm, etc)	*	*	*	*	*	*	*	*		*
The computer on which the infection was found	*	*	*	*	*	*	*	*	*	*
The user who was logged on at the time the infection was detected	*		*	*	*		*	*	*	*
The action and current status of the infection (i.e. cleaned, deleted, quarantined, still infected)	*	*	*	*	*	*	*	*	*	*
The current location of the infected file (i.e. local quarantine)	*	*	*	*	*	*	*	*	*	*
The scan that detected the infection (i.e. On Access, Manual, Start-up, etc)	*	*	*	*	*		*	*		*
End-user Interaction										
Let the end-user choose the action	*	*	*	*	*	*	*	*	*	
Notify the end-user										
By displaying a pop up or balloon	*	*	*	*	*	*	*	*	*	*
Silen mode	*	*	*	*	*	*	*	*	*	*
By adding a warning to an infected email body or subject (email) and by replacing an infected attachment	*	*	*	*	*	*	*		*	*
Run a script or application after detection	*		*				*			
Can a second or alternative action be defined (i.e. if the first action fails)?		*	*	*	*		*	*	*	*
Which file specific actions can the product perform?										
Clean / Delete	*	*	*	*	*	*	*	*	*	*
Can the product create a backup of the file before attempting to clean it?	*	*	*			*	*	*	*	*
Quarantine on the local system	*	*	*	*	*	*	*	*	*	*
Quarantine in a central location		*	*	*	*		*			*
Deny Access	*	*	*	*	*	*	*	*	*	*
Which processes specific actions can the product perform										
Terminate the process	*	*	*	*	*	*	*	*	*	*
Stop the service	*	*	*		*			*	*	*

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G DATA	Ikarus	Kaspersky Lab	McAfee	Sophos	Symantec
Does to product provide preconfigured conditions?										
Preconfigured Antivirus Check	*	*	*			*	*		*	*
Preconfigured Firewall Check	*	*	*				*		*	*
Preconfigured Patch Management Check			*	*			*		*	*
Other			Operating system patching status check				database update			
Remediation										
Does the product provide remediation capabilities?		*	*	*	*	*	*	*	*	*
Which remediation action can be defined in the user interface (without resorting to scripts)?										
Registry remediation		*		*			*	*	*	*
File remediation										
Delete files / folders		*	*	*		*	*	*	*	*
Download files							*	*	*	*
Process remediation										
Run service / application in user / system security context			*					*	*	*
Software Remediation										
Download software and patches				*	*		*			*
Install / uninstall software and patches in user / system security context				*	*		*	*	*	*
End-user interaction										
Inform user		*	*	*	*	*	*	*	*	*
Query user			*	*	*		*		*	*
Enforcement										
Can the product prevent that a client failing the client health check connects to a network?				*			*			*
Behaviour detection										
Behavior detection	*	*	*	*	*	*	*	*	*	*
Is this technology enabled by default?	*	*	*	*		*	*	*	*	*
General capabilities										
Is the firewall stateful for TCP and UDP connections?		*	*	*	*		*	*	*	*
Can the firewall analyze VPN traffic		*					*		*	*
Firewall Rules										
Does the product come with default policies?										
For workstations		*	*	*	*		*	*	*	*
For server				*	*		*	*		*
Protocol										
TCP/UDP/ICMP		*	*	*	*		*	*	*	*
Raw Ethernet		*	*				*	*	*	*
Other		Any other IP protocol is supported	IPv6-ICMP, IGMP, GRE, ESP, SMP		IGMP, GGP, GUP, IDP, GRE					
Which Actions can be taken when a firewall rule is triggered?										
Allow / Block traffic / Ask / notify the end-user when traffic is blocked		*	*	*	*		*	*	*	Allow, Block, Ask and Notify are all allowed
Log										
Log the incident		*	*	*	*		*	*	*	*
Include packet data in log				*						*

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G DATA	Ikarus	Kaspersky Lab	McAfee	Sophos	Symantec
Is there a web based console?					*		*	*		*
Administrator Management										
Rights / Access Control										
Does the product support multiple administrators and different access levels?	*	*	*	*	*		*	*	*	*
Authentication mechanism										
Can administrators be authenticated using an integrated authentication mechanism (i.e. username / password)?	*	*	*	*	*	*	*	*	*	*
Does the product enforce minimum password lengths and maximum password age?		*		*	*		*	*	*	*
Can administrators be authenticated using Active Directory?			*		*		*	*	*	*
Account Security										
Does the product log an administrator out after being idle for some time?		*			*		*	*	*	*
Administrator Auditing										
Does the product keep an audit log?		*	*	*		*	*	*		*
Device Control										
Does the product allow administrators to limit the use of external devices (USB sticks, printers, etc)?			*	*	*		*		*	*
Failover										
What if the AV Server (local) hangs up										
automatic switching to a second local server		*	*		*		*	*	*	*
updates from vendor-server instead of local server	*	*	*	*	*	*	*	*	*	*
other			Log and notifications	Multiple proxy servers and proxy chaining supported		service is automatically restarted	any other network shared folder			
Quarantine										
Quarantine Folder										
Is there a centralized quarantine-folder			*	*	*					*
Is there a quarantine-folder on the client	*	*	*	*	*	*	*	*		*
can administrators specify the location of the quarantine folder anywhere	*		*	*			*	*		
rechecking quarantine										
after an signature update, is the quarantine folder checked?		*			*	*	*	*	*	*
automatically		*				*	*	*	*	*
manual	*	*			*		*	*		
undo av-action if false positive is detected	*	*	*			*	*	*		*
Messaging										
Exchange										
Feature overview Messaging										
Modules and functional areas		Monitoring, SMTP Groups, Antivirus, Antispam, Content filtering, Attachment filtering, Update	Product for Exchange. Full integration with MS Exchange, scans the whole Exchange store and Antispam Protection. Managable from the central management server. Supports 64-bit Exchange.	Transport and storage AV scanning, Spam Control, attachment filtering, intelligent file type recognition, keyword-based content filtering, zero-day protection, centralized quarantine management	Transport and storage AV Scanning and extendable by a MailSecurity Gateway					Integrated option with MS Exchange and Domino. Secure email gateway option (virtual or physical appliance) for Enterprise Edition. Antispam, antivirus, antiphishing, content filtering, and data loss prevention
Malware detection										
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled	*	*	*	*	*		*			*

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G DATA	Ikarus	Kaspersky Lab	McAfee	Sophos	Symantec
Information Store scan on every server	*	*	*	*	*		*		*	*
Support of automatic virus pattern updates	*	*	*	*	*		*		*	*
Scanning of e-mail message text and attachments	*	*	*	*	*		*		*	*
Definition of file limitations by a combination of file name, file extension and file size		*	*		*		*			*
Application of the restrictions on file archives	*	*	*	*	*		*		*	*
Automatic detection of new mailboxes	*	*	*	*	*		*		*	*
Scanning of existing mailboxes	*	*	*	*	*		*		*	*
Anti-Spam										
scan according to the company's policies on prohibited, not desirable or confidential content	*	*	*	*			*		*	*
Blocking unwanted e-mail senders (spam senders, mailing lists, etc.) as well as to unwanted recipients (e.g. competitors)	*	*	*	*			*		*	*
Analysis of images on undesirable content (e.g. pornography)		*	*	*			*			
Using current spam pattern for the fast detection of new spammer tricks	*	*	*	*	*		*		*	*
User-Specific Management of White- and blacklists on the server solely for effective blocking unwanted e-mails	*	*	*				*		*	*
Definition of transmitter / receiver channels on a dedicated e-mail communications	*		*				*			
Freely editable exclusion list for addresses and content in subject and message text	*	*	*			*	*		*	*
Flexible notifications of blocked e-mails (directly or schedule) to administration or transmitter/receiver email	*	*	*	*			*		*	*
User-specific access to e-mails in the quarantine	*		*				*		*	*
Centralized quarantine management	*	*	*	*			*		*	*
Formation of company-specific e-mail categories	*		*				*			*
Automatic classification of e-mails to one or more categories	*	*	*				*			*
Response Management through defined classifications, for example, the customer support automatic forwarding of e-mails to qualified employees		*	*				*			*
Document protection: Following categories may, for example, all outgoing e-mails on company-related content should be examined							*		*	*
A content audit of e-mail attachments is also possible	*		*				*		*	*
if the same mail is delivered several times, would it be blocked as spam		*	*				*			
Feature overview Messaging										
General Windows										
Modules and functional areas			Integration with most Windows mail servers is possible through the command line scanner		Gateway solution, Exchange Plugin for Exchange 2007/2010/2013 or combination of both					Integrated option with MS Exchange and Domino. Secure email gateway option (virtual or physical appliance) for Enterprise Edition. Antispam, antivirus, antiphishing, content filtering, and data loss prevention
Malware detection										
Recursive scan of all e-mails and file attachments in real time, event-and time-controlled	*		*	*	*	*	*			*
Information Store scan on every server	*		*	*	*		*		*	*
Support of automatic virus pattern updates	*		*	*	*	*	*		*	*
Scanning of e-mail message text and attachments	*		*	*	*	*	*		*	*
Definition of file limitations by a combination of file name, file extension and file size	*		*	*			*			*
Application of the restrictions on file archives such as zip, rar	*		*	*	*	*	*			*
Automatic detection of new mailboxes	*		*	*	*	*	*		*	*

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G DATA	Ikarus	Kaspersky Lab	McAfee	Sophos	Symantec
Scanning of existing mailboxes	*		*	*	*	*	*		*	*
Language:										
In which languages are your business/corporate products available?	German, English, Italian, Japanese, Turkish, Spanish, Portuguese, French, Russian, Dutch, Chinese Korean	English, French, Spanish, German	Management Server and Console: English, Japanese, German, Russian, French, Spanish, Polish, Chinese, Portuguese, Italian. Client: Bulgarian, Chinese, Croatian, Czech, Danish, Dutch, English, Estonian, Greek, Hungarian, Italian, Finnish, French, German, Hungarian, Italian, Japanese, Kazakh, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Latin, Slovak, Slovenian, Spanish, Swedish, Thai, Turkish, Ukrainian, Lithuanian.	Chinese, Czech, Danish, Dutch, English, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish	German, English, Italian, Spanish, French, Russian, Polish, Turkish, Portuguese, Chinese, Japanese	German, English, Italian, Russian, Turkish	English, French, German, Japanese, Chinese, Russian, Spanish, Portuguese, Polish, Turkish, Arabic, Italian	English, Portuguese, Chinese, Dutch, French, German, Hebrew, Italian, Japanese, Korean, Polish, Spanish, Swedish, Russian	English, French, German, Italian, Japanese, Spanish, Chinese	English, Chinese, Korean, French, Italian, German, Spanish, Portuguese, Russian, Czech, Polish, Japanese
In which languages are your (help) manuals available?	German, English		All	English, German, Spanish, French, Japanese, Finnish, Italian, Swedish.	German, English, Italian, Spanish, French, Polish	German, English				
Support										
24/7/365 phone support	*	*	*	*	*		*	*	*	*
Supported Support Languages	German, English, Italian, Japanese, Turkish, Spanish, Portuguese, French, Russian, Dutch, Chinese Korean	English, French, Spanish, German	All	English, Danish, Finnish, French, German, Cantonese, English, Japanese, Norwegian, Swedish	German, English, Italian, Spanish, French	German, English	All	English, Portuguese, Chinese, Dutch, French, German, Hebrew, Italian, Japanese, Korean, Polish, Spanish, Swedish, Russian	English, French, German, Spanish, Italian, Japanese, Chinese	English, French, German, Italian, Spanish, Portuguese, Czech, Polish, Russian, Chinese, Korean, Japanese, Taiwanese
Remote Desktop Control for support	*	*	*		*	*	*	*	*	*
Support per Forum	*	*	*	*			*	*	*	*
Support over Email	*	*	*	*	*	*	*	*	*	*
On-Site service?		*	*	*	*	*	*	*		*
Service										
Managed by Vendor, this means, can the whole management process be done as a service by the vendor?	*	*	*	*	*			*	*	*
Pricing (may vary)										
Scenario A: 5 clients, server, outlook as mail client										
recommended product	Avira Endpoint Security	Small office Security by Bitdefender	ESET Endpoint Antivirus	F-Secure Business Suite	G DATA Small Business Security	IKARUS anti.virus	Kaspersky Small Office Security	McAfee Small Business Security	Sophos Endpoint Protection - Business	Symantec Endpoint Protection Small Business Edition
1 year Euro	193	202	150	306	167	34	132	196	214	162
3 years Euro	385	403	317	128	467	55	301	343	428	389
1 year USD	250	246	192	306	167	44	229	210	244	175
3 years USD	500	491	402	765	467	70	498	367	488	419
Scenario B SMB: 1 SBS 2003 Server, 25 Clients										
recommended product	Avira Small Business Security Suite	Small office Security by Bitdefender	ESET Endpoint Antivirus + ESET File Security	F-Secure Business Suite	G DATA Endpoint Protection Business	IKARUS security.manager	Kaspersky Small Office Security	McAfee Small Business Security	Sophos Endpoint Protection - Business	Symantec Endpoint Protection Small Business Edition
1 year plan EURO	1 260	785	473	942	753	910	744	1 610	656	300
3 year plan EURO	2 520	1 570	993	2353	1 530	1 456	1 674	3 170	1312	692

Feature list	AVIRA	Bitdefender	ESET	F-Secure	G DATA	Ikarus	Kaspersky Lab	McAfee	Sophos	Symantec
1 year plan USD	1 638	958	601	942	753	1 170	985	1 509	731	316
3 year plan USD	3 276	1 916	1262	2353	1 530	1 871	2 313	3 169	1487	991
Scenario C: 1 Fileserver, 1 Exchange server, 200 Clients										
recommended product	Avira Business Security Suite	Small office Security by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G DATA Endpoint Protection Business + MailSecurity + ClientBackup	IKARUS security.manager	Kaspersky Endpoint Security + Kaspersky Security for Mail Server	McAfee Small Business Security	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition
1 year plan EURO	7 620	8 199	4 815	4 842	6 624	5 454	5 158	6 738	3 950	5 292
3 year plan EURO	15 240	16 399	10 113	12 104	14 112	8 726	11 607	11 861	7 900	10 079
1 year plan USD	9 906	10 046	6 122	4 842	6 624	7 009	5 838	8 005	4 500	4 944
3 year plan USD	19 812	20 092	12 856	12 104	14 112	11 214	11 677	14 089	9 000	9 310
Scenario D, 2 Fileserver, 1 Exchange server, 1000 Clients										
recommended product	Avira Business Security Suite	Small office Security by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G DATA Endpoint Protection Business + MailSecurity + ClientBackup	IKARUS security.manager	Kaspersky Endpoint Security + Kaspersky Security for Mail Server	McAfee Endpoint Protection Suite	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition
1 year plan EURO	21 300	29 850	15 821	15 857	23 040	19 057	18 617	28 545	18 000	27 075
3 year plan EURO	42 600	59 700	33 244	39 638	47 520	30 491	41 899	50 240	27 000	61 563
1 year plan USD	27 690	36 387	20 111	15 857	23 040	24 492	22 389	32 939	20 250	20 060
3 year plan USD	55 380	72 774	42 260	39 638	47 520	39 187	44 767	57 973	40 500	44 579
Scenario E: 10 Fileserver, 10 Exchange server, 10000 Clients										
recommended product	Avira Business Security Suite	Small office Security by Bitdefender + Bitdefender Security for Exchange	ESET Endpoint Antivirus + ESET File Security + ESET Mail Security	F-Secure Business Suite	G DATA Endpoint Protection Business + MailSecurity + ClientBackup	IKARUS security.manager	Kaspersky Endpoint Security + Kaspersky Security for Mail Server	McAfee Endpoint Protection Suite	Sophos Endpoint Protection - Business	Symantec Protection Suite Enterprise Edition
1 year plan EURO	136 000	259 254	116 084	81 763	230 400	120 240	186 170	162 224	180 000	220 820
3 year plan EURO	272 000	518 508	243 176	204 408	475 200	192 384	418 990	285 470	270 000	530 030
1 year plan USD	176 800	316 239	147 566	81 763	230 400	154 530	223 890	187 174	202 500	159 960
3 year plan USD	353 600	632 477	309 125	204 408	475 200	247 251	447 670	329 357	405 000	388 788

Copyright and Disclaimer

This publication is Copyright © 2014 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (October 2014)