# IT Security Products for Small Business

# Review of IT Security Suites for Small Business, 2015

Language: English

September 2015
Last revision date: 1st October 2015

**www.av-comparatives.org**

# Contents

## Introduction

AV-Comparatives' 2015 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 Website[1], 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.

We have used 64-bit Windows 7 Professional SP1 as a test client for all products; additionally, we have tested a 64-bit Windows 10 Pro client where this OS is supported by the vendor. 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 companies with 25 users or less that 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. The *Status* and Warnings sections both relate to monitoring the most important protection functions and alerting the administrator if any of these are not as they should be. We feel that one of the most important items here is the status of real-time protection (RTP). This may be deactivated for a number of reasons: malware, hard disk defect, Windows failing to load a service, or a user with administrator rights switching it off. We feel that the console should show an alert if RTP is not active, regardless of how the situation came about. For products that include their own client firewall in the endpoint protection software, the above point would apply to this as well. Other important items that should be monitored include the date/time of the most recent malware-signature update, and any unresolved malware detections (if malware has been successfully dealt with by the client software and no further action is required, we feel this should be logged, but does not need an alert).

### Supported operating systems

Here we list Windows Server, Windows client and Mac OS X clients supported by the product. Details of supported mobile operating systems (Android and iOS), which we have not covered in the review, can be found in the product's feature list at the end of the document.

[1] http://www.microsoft.com/en-us/server-cloud/products/windows-server-2012-r2-essentials/comparison.aspx

## Documentation

We have looked at the external documentation, i.e. manuals and online knowledge base (as opposed to the console's built-in help features). These could be used to help install the console where applicable, whereas a help feature built into the console obviously could not.

## Management Console

### Installation and configuration

How to set up the console so that the administrator can proceed with deploying endpoint protection software to clients.

### Layout

Console design, with emphasis on finding major features.

### Preparing devices for deployment

Is it necessary to configure either the management server or the clients, e.g. by opening firewall ports or enabling file sharing, to enable deployment and management?

### Deploying the endpoint protection software

Deployment methods available, e.g. remote push, emailing a link to users, local installation on the client itself.

### Monitoring the network

*Status*

How does the console show overall security status of the network, i.e. what proportion of clients are functioning as they should, and what proportion have a problem of some sort?

*Warnings*

How does the console alert the administrator to the details of problems on individual machines, e.g. client out of date, unresolved malware detection, protection disabled?

*Rectifying problems*

What mechanism does the console provide for fixing the problems shown in an alert – e.g. reactivating a component, running a scan or update?

*Malware alerts*

How does the console display malware detections?

*Program version*

Which version of the client software is currently installed on each device?

### Managing the network

*Scanning*

How to run on-demand malware scans on protected devices.

*Scheduling Scans*

How to set up a regular scheduled scan.

### *Updates*

How to bring malware definitions on clients up to date.

### *Removing devices from the console*

If a device is lost, stolen or decommissioned, how can its entry be deleted?

### Integrated help feature

Details of the console's built-in help feature and how to access this.

## Respective endpoint protection programs for Windows and Mac OS X clients

### Installation

What steps are involved, and what options/choices are there?

### Main program window

Are standard features such as status, updates, scans and help easy to find?

### System Tray icon

What functions can be accessed from the Windows/Mac OS System Tray icon?

### Unauthorised access

If a user logs on to the computer with a standard user account, i.e. without administrator privileges, is it possible to disable real-time protection?

### Malware alerts

What sort of alert is shown if the EICAR test file is downloaded?

### Windows Security Center/Windows Defender

For Windows clients only, we have also looked at whether the program registers as antivirus/antispyware/firewall in the Windows Security Center/Action Center/Security and Maintenance applet, and whether Windows 7's Windows Defender is disabled.

## Windows server protection software

How are the main functions – status, update and scans – shown?

## Summary

Could the console be installed by a non-expert administrator, or would it be better for a small business to employ an IT professional to set it up? Once up and running, how easy would it be for a non-expert to manage the network with the console?

## Console types

There are three main types of management console covered in this review.

**Cloud-based consoles** run on the manufacturer's servers. They can be accessed from any web browser on any Internet-connected device, by going to the URL provided by the manufacturer and logging in with the appropriate credentials. They have the advantages for small businesses that no installation of the console is required, and that deployment of the client software is normally very straightforward for non-expert administrators.). Additionally, a device can be monitored and managed easily wherever it is in the world, as long as it is connected to the Internet; this is obviously very useful for businesses with staff who frequently work outside of the office and are thus not connected to the company LAN.

**Server-based consoles** run on the company's own internal server (Windows or Linux) on the LAN. Generally speaking, small businesses are likely to need an IT professional to install the product. The user interface component of the program may be integrated into the program that runs on the server, available as a separate component that can be installed on the administrator's desktop or laptop PC, or accessible by web browser if a suitable HTTP server-function has been set up by the server component. Client-software deployment options may include those available for cloud-based consoles, with an additional option of remote push installation for devices connected to the company LAN. In this case, some configuration of client devices is usually necessary (such as enabling file sharing), after which the endpoint protection software can be sent out to multiple clients at once from the administration console. Server-based consoles may offer greater functionality than cloud-based ones, and some admins may prefer to have the system completely under their own control. Management of devices outside the LAN would require e.g. a VPN to be set up, however.

**Virtual-appliance-based consoles** are a variety of server-based console, in which the manufacturer provides a pre-configured virtual machine, usually Linux-based, which is imported into a common virtualisation platform. For an IT Professional accustomed to working with virtual machines, the virtual-appliance method has the advantage of quick and easy installation and configuration. Aside from this, the pros and cons of server-based consoles apply.

## 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 2015). The products tested for the review are listed below:

- Bitdefender Endpoint GravityZone
- ESET Remote Administrator
- F-Secure Protection Service for Business
- G DATA AntiVirus Business
- Kaspersky Small Office Security
- McAfee SaaS Endpoint Protection
- Sophos Endpoint Security and Control Cloud
- Symantec Endpoint Protection
- Trend Micro Worry-Free Business Security Services

## AV-Comparatives Approved Business Product Award 2015

This year, we are once again pleased to report a very high overall standard, and that all the products reviewed receive our Approved Business Product award.

# Management Summary

We have grouped the products according to the type of management console reviewed, namely cloud-based console, server-based console, and virtual-appliance-based console. Individual products are listed alphabetically within their respective group.

### Cloud-based consoles

**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.

**Kaspersky Small Office Security** is an outstanding choice for a small business without full-time IT support. The very simple and clean design of the console is ideal for someone new to security-management consoles and makes the essentials especially easy to access. Endpoint protection is very familiar and easy to use, and help facilities are excellent.

**McAfee SaaS Endpoint Protection** is a very suitable product for smaller businesses, with security status being clearly displayed in an easy-to-navigate, customisable console. Client software can be installed very simply and has a clear and familiar interface.

**Sophos Endpoint Security and Control Cloud** includes some innovative features, such as the automatic reactivation or reinstallation of disabled or uninstalled client software. There is also Tamper Protection, which protects client software against unauthorised access. The console is clean and easy to navigate, and client deployment very simple.

**Trend Micro Worry-Free Business Security Services** uses a clear, modern design for all components of the product. The default status page of the console provides an at-a-glance view of network security, while most other monitoring and management tasks can be carried out from a single page. Non-expert admins should be able to install and manage clients without any difficulty.

### Server-based consoles

**G Data Antivirus Business** is very easy for an experienced administrator to install, with e.g. seamless integration of SQL Express into the setup wizard. The console is reminiscent of the familiar Microsoft Management console, and could comfortably be used by a non-expert admin to manage the network. The excellent manual could be used to assist if necessary. Client software is minimalist by default, but admins can allow users to carry out basic tasks if they want.

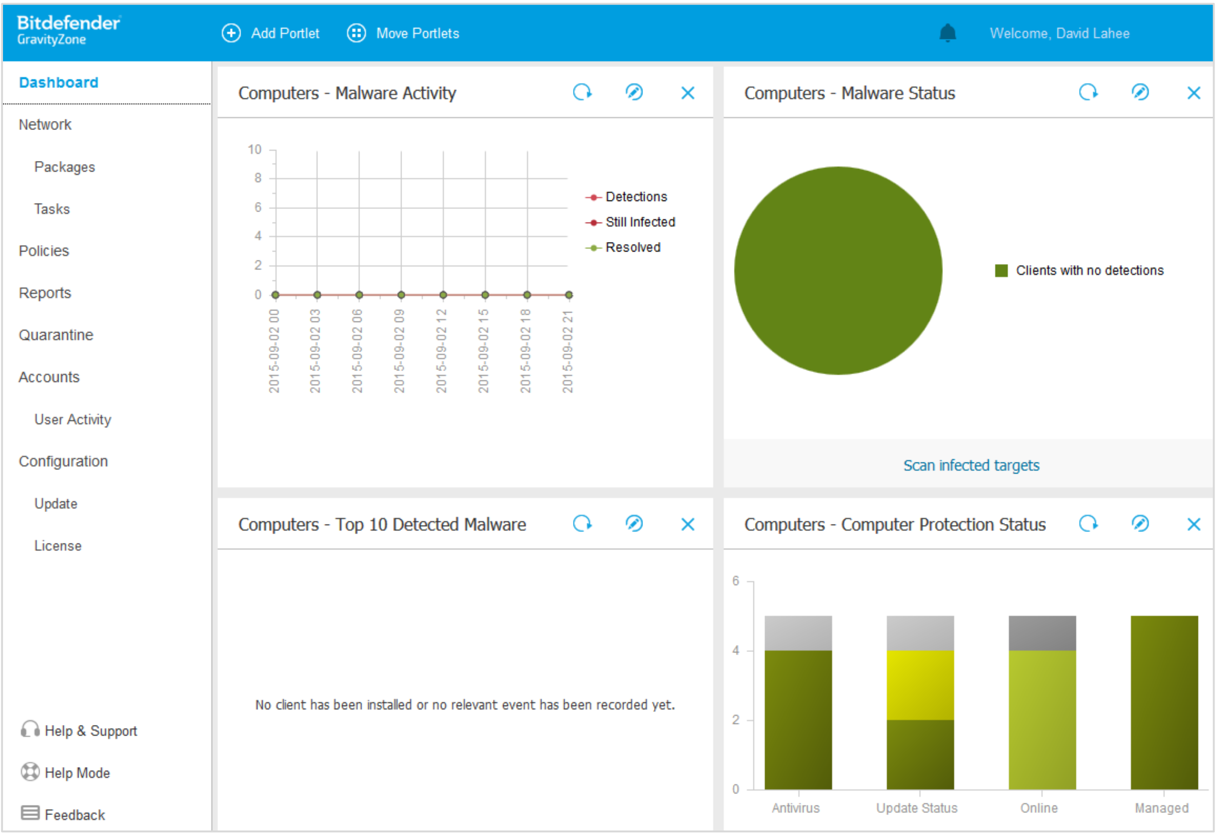
**Symantec Endpoint Protection** can cope comfortably with larger networks, but could nonetheless be used by small businesses. Installation of the console is extremely simple, while deployment, monitoring and management of clients should not prove challenging even to inexperienced admins. Client software is practical and familiar, and documentation comprehensive.

### Virtual-appliance-based consoles

**Bitdefender GravityZone** is very straightforward to set up for an experienced administrator, and provides useful integrated quick-start pages and well-produced manuals. The console is clean and well-designed, as is the client software.

**ESET Remote Administrator** could be installed on a Windows or Linux server, in addition to the virtual-appliance variant. Whichever option is chosen, the console is powerful and could comfortably cope with bigger networks. We quickly felt at home with the monitoring and management interface, and feel that non-expert administrators would need minimal initial training. The client software is very user-friendly, while documentation and help features are outstanding.

## Bitdefender GravityZone Business Security



No client has been installed or no relevant event has been recorded yet.

### Introduction

Bitdefender provides a range of business products for large and small companies. For this review, we tested GravityZone Business Security, which uses a cloud-based or on-premise console to manage protection software on client devices. We tested the on-premise version, which is provided in the form of a pre-configured, Ubuntu-based virtual hard disk, with appropriate versions for all popular virtualisation platforms, including VMWare, Citrix Xen and Microsoft Hyper-V. From a license perspective the product supports two license types. Additional features[2] are available in the Advanced Business Security package.

### Software versions reviewed

Bitdefender Endpoint Security Tools for Windows 6.2.4.612
Bitdefender Endpoint Security for Mac 3.3.9160

### Supported operating systems

Windows clients: Windows 10, 8, 8.1, 7, Vista, Windows XP
Windows servers: Windows Server 2012/R2, 2008/R2, 2003/R2; Windows Small Business Server 2011, 2008, 2003; Windows Home Server
Mac clients: Mac OS X Lion (10.7.x), Mountain Lion (10.8.x), Mavericks (10.9.x), Yosemite (10.10)
Linux[3]
Both hardware and virtualised systems are supported in all cases.

[2] http://www.bitdefender.com/business/#compare
[3] http://www.bitdefender.com/business/advanced-security.html

## Documentation

### Manuals

Bitdefender produce two manuals for the product. There is a 95-page Installation Guide, which covers configuration of the virtual appliance, accessing the console, plus deployment and maintenance of client software. There is also a very comprehensive 318-page Administrator's Guide, covering all aspects of the software.

### Knowledge base

There is an online Support Center, which we would describe as a searchable FAQ section.

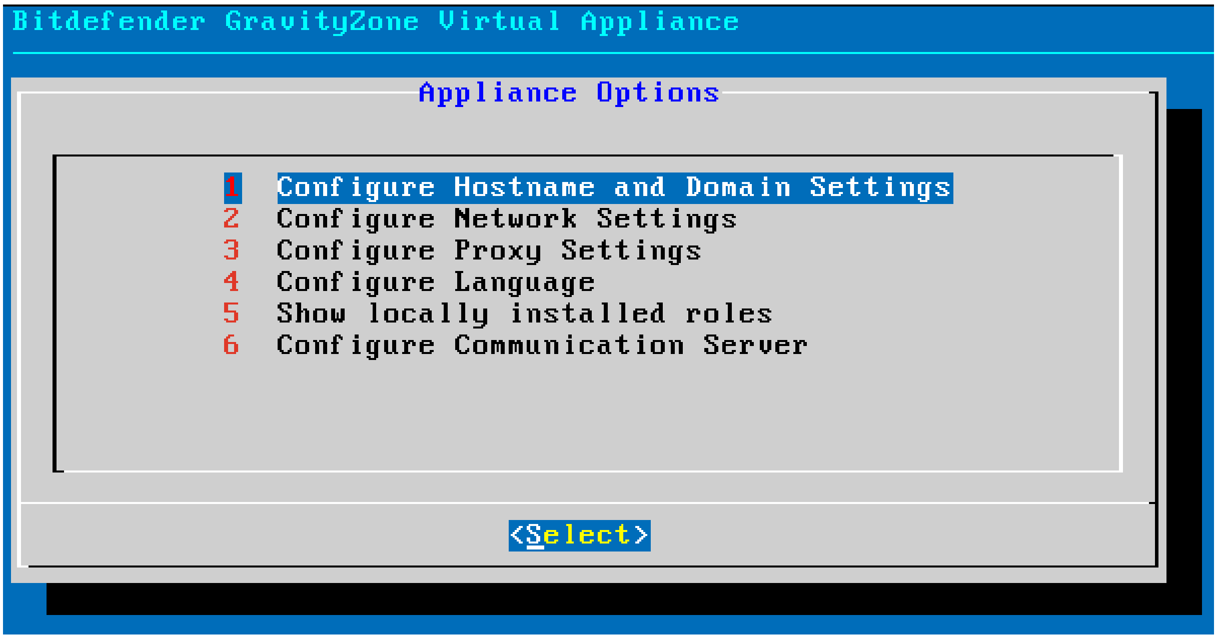
### Comment

We found both manuals to be of a very high standard. They are clearly written, well illustrated with screenshots, and easy to navigate.

## Management Console

### Installation and configuration

We used VMWare Workstation as the virtualisation platform in our test, and consequently downloaded the .OVA virtual hard drive, which is compatible with this. Instructions for importing .OVA files are provided on the VMWare knowledge base;[4] we found the process is very quick and easy. When the virtual machine is first started, the user has to set a password for administrator access, and configure the TCP/IP settings via a semi-graphical interface reminiscent of the initial phase of Windows XP setup:

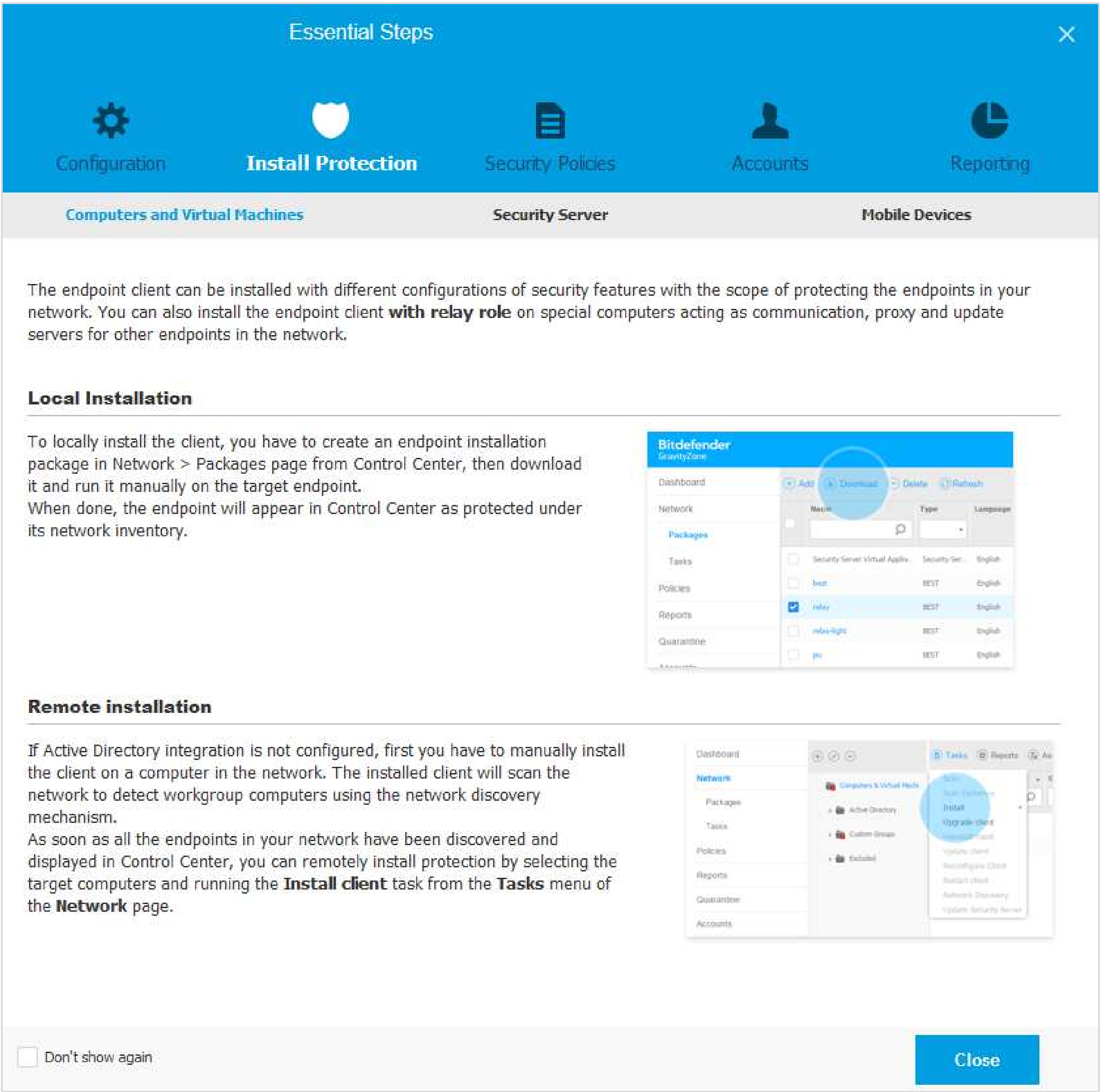


```
Bitdefender GravityZone Virtual Appliance

                 Appliance Options

        1  Configure Hostname and Domain Settings
        2  Configure Network Settings
        3  Configure Proxy Settings
        4  Configure Language
        5  Show locally installed roles
        6  Configure Communication Server

                     <Select>
```

The console can then be accessed from Windows or Mac OS X computers by typing the VM's IP address into a browser. The admin has to create a Bitdefender account, or log in with an existing one, and create a username and password for the console itself. It transpires that a complex password is needed, although this is not stated, and the admin has to use trial and error to find a password that is accepted.

[4] http://pubs.vmware.com/workstation-10/index.jsp?topic=%2Fcom.vmware.ws.using.doc%2FGUID-DDCBE9C0-0EC9-4D09-8042-18436DA62F7A.html

Having successfully logged in, the admin then sees a number of informative welcome pages, called *Essential Steps,* which explain the product and its use. An example is shown below:



The endpoint client can be installed with different configurations of security features with the scope of protecting the endpoints in your network. You can also install the endpoint client **with relay role** on special computers acting as communication, proxy and update servers for other endpoints in the network.

**Local Installation**

To locally install the client, you have to create an endpoint installation package in Network > Packages page from Control Center, then download it and run it manually on the target endpoint.
When done, the endpoint will appear in Control Center as protected under its network inventory.

**Remote installation**

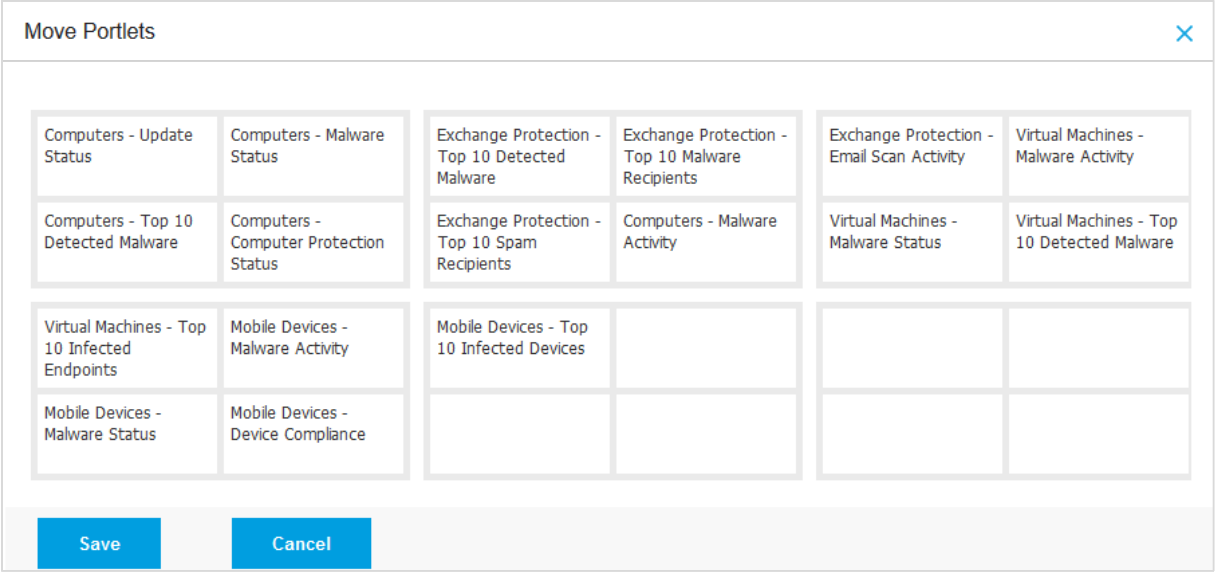
If Active Directory integration is not configured, first you have to manually install the client on a computer in the network. The installed client will scan the network to detect workgroup computers using the network discovery mechanism.
As soon as all the endpoints in your network have been discovered and displayed in Control Center, you can remotely install protection by selecting the target computers and running the **Install client** task from the **Tasks** menu of the **Network** page.

□ Don't show again

The section has a *Don't show again* checkbox to allow it to be skipped at the next logon.

## Layout

The console consists of a left-hand menu column, from which major functions such as policies, reports and quarantine can be accessed. By default, the main area of the console shows 4 panels with protection status and malware activity information. We note that this can be very easily customised by clicking *Move Portlets* at the top. This opens the following configuration dialog, which lets the admin move the panels ("portlets") from page to page by dragging and dropping:



| | | | | | |
|---|---|---|---|---|---|
| Computers - Update Status | Computers - Malware Status | Exchange Protection - Top 10 Detected Malware | Exchange Protection - Top 10 Malware Recipients | Exchange Protection - Email Scan Activity | Virtual Machines - Malware Activity |
| Computers - Top 10 Detected Malware | Computers - Computer Protection Status | Exchange Protection - Top 10 Spam Recipients | Computers - Malware Activity | Virtual Machines - Malware Status | Virtual Machines - Top 10 Detected Malware |
| Virtual Machines - Top 10 Infected Endpoints | Mobile Devices - Malware Activity | Mobile Devices - Top 10 Infected Devices | | | |
| Mobile Devices - Malware Status | Mobile Devices - Device Compliance | | | | |

The group of 4 portlets in the top left-hand corner is shown by default when the console is first opened; the admin can customise this so that the items he/she feels are most important can be shown here.

## Preparing devices for deployment

We did not need to pre-configure client or server devices before installation.

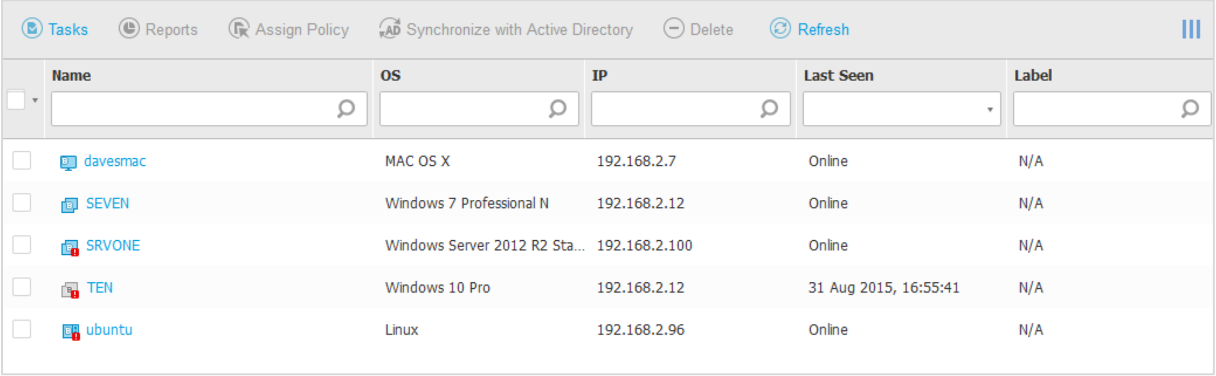
## Deploying the endpoint protection software

As explained in the welcome page shown above, the client software can be deployed by local installation or remote push installation; we used the former on our test network.

## Monitoring the network

### *Status*

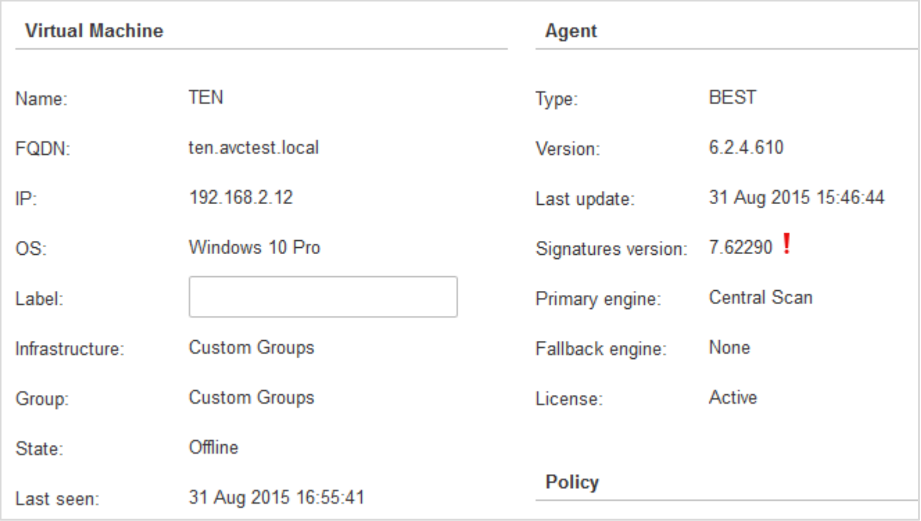
An overview of system security status is shown in the bottom-right panel of the Dashboard. For a more detailed view, the administrator can click on *Network* at the top of the menu column on the left, then the relevant group of computers; this displays details of individual devices:



| | Name | OS | IP | Last Seen | Label |
|---|---|---|---|---|---|
| □ | davesmac | MAC OS X | 192.168.2.7 | Online | N/A |
| □ | SEVEN | Windows 7 Professional N | 192.168.2.12 | Online | N/A |
| □ | SRVONE | Windows Server 2012 R2 Sta... | 192.168.2.100 | Online | N/A |
| □ | TEN | Windows 10 Pro | 192.168.2.12 | 31 Aug 2015, 16:55:41 | N/A |
| □ | ubuntu | Linux | 192.168.2.96 | Online | N/A |

### *Warnings*

As shown above, devices with a problem are marked with an exclamation mark in a red box. Clicking on an individual machine displays detailed information for that device, including the reason for the warning:



| Virtual Machine | | Agent | |
|---|---|---|---|
| Name: | TEN | Type: | BEST |
| FQDN: | ten.avctest.local | Version: | 6.2.4.610 |
| IP: | 192.168.2.12 | Last update: | 31 Aug 2015 15:46:44 |
| OS: | Windows 10 Pro | Signatures version: | 7.62290 ! |
| Label: | | Primary engine: | Central Scan |
| Infrastructure: | Custom Groups | Fallback engine: | None |
| Group: | Custom Groups | License: | Active |
| State: | Offline | | |
| Last seen: | 31 Aug 2015 16:55:41 | Policy | |

### *Rectifying problems*

To rectify the out-of-date signatures shown in our test device above, we ran *Update client* from the *Tasks* menu on the network overview page. To re-enable real-time protection after deliberately disabling it, we re-applied the default policy; we were impressed to see that this reactivated protection on the client in less than a minute.

### *Malware alerts*

If the client software detects and successfully blocks malware, this is not shown in the security status, but can be seen in the *Malware Activity* portlet. Admins can however use the *Reports* function to quickly display details of successful malware detections on all machines.

### *Program version*

This is shown in the properties page of individual devices (see screenshot above).

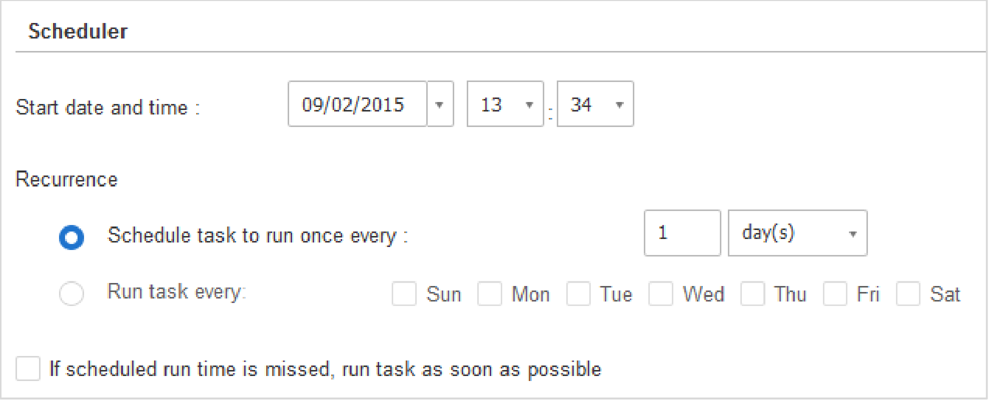
## Managing the network

### *Scanning*

Scans can easily be run by selecting clients in the group overview page and selecting *Scan* from the *Tasks* menu. Admins should be careful not to select the Linux machine on which the console is running, as in this case the *Tasks* menu will be greyed out.

### *Scheduling Scans*

Scans can be scheduled by going to *Policies, Add, Antimalware, On-Demand, Add* and then selecting a quick, full or custom scan as appropriate; the dialog box that opens allows a schedule to be set:



Scheduler

Start date and time : 09/02/2015 ▾ 13 ▾ : 34 ▾

Recurrence

● Schedule task to run once every : 1 day(s) ▾

○ Run task every: □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

□ If scheduled run time is missed, run task as soon as possible

### *Updates*

These can be run from the *Tasks* menu on the overview page for the group concerned.

### *Removing devices from the console*

The overview page includes a *Delete* button in the toolbar at the top.

### Integrated help feature

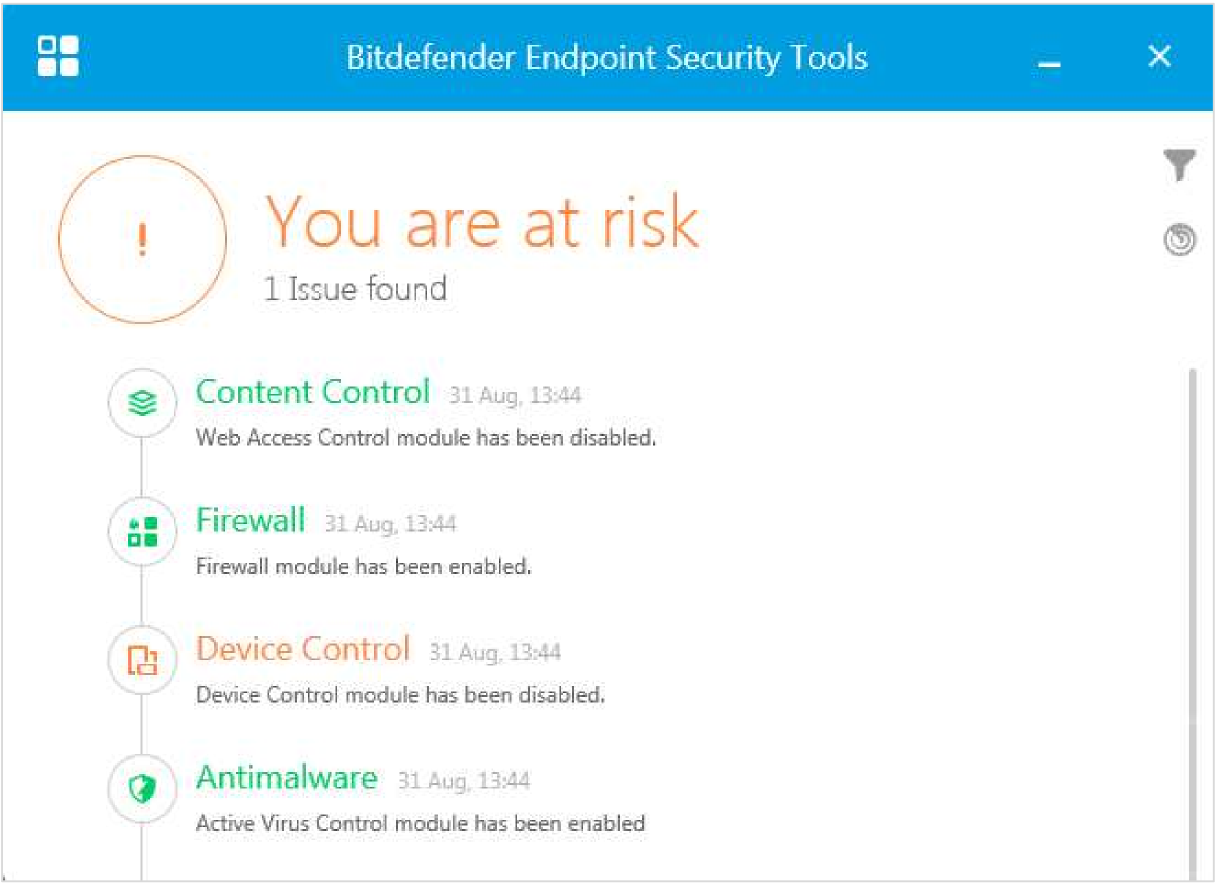
Clicking *Help & Support* in the bottom left-hand corner, then *Essential Steps* opens the welcome pages described in the INSTALLATION AND CONFIGURATION section above.

### Comment

We would definitely advise small businesses using GravityZone to have an IT consultant do the initial setup and configuration of the virtual appliance. However, for a professional who is familiar with the relevant virtualisation software and the essentials of TCP/IP network technology, this is a very straightforward procedure. Because the virtual machine has been pre-configured, we do not feel that any particular knowledge of Linux is required.

We found the simple layout of the console, with essentially just one menu panel at the side, to be easy to navigate. We particularly liked the ability to customise the content of the Dashboard, and the simple drag-and-drop method used to do this.

## Windows client protection software



Bitdefender Endpoint Security Tools

You are at risk

1 Issue found

Content Control 31 Aug, 13:44

Web Access Control module has been disabled.

Firewall 31 Aug, 13:44

Firewall module has been enabled.

Device Control 31 Aug, 13:44

Device Control module has been disabled.

Antimalware 31 Aug, 13:44

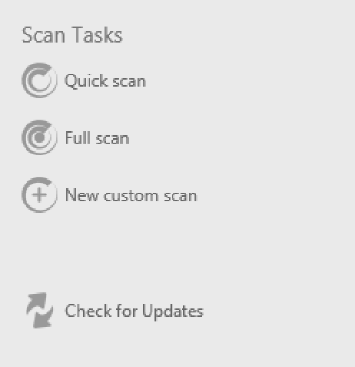
Active Virus Control module has been enabled

### Installation

The admin downloads and runs the relevant installer from the console. There is literally nothing else to do except click *Finish* at the end, making it the simplest setup wizard imaginable.

### Main program window

The program window features a main status display at the top, with additional status items for individual components. Clicking the circular icon in the top right-hand corner of the window opens a panel from which updates and scans can be started:



### Windows Security Center/Windows Defender

Bitdefender Endpoint Security registers as antivirus, antispyware, and (in the default configuration) firewall with Windows Security Center.

### System Tray icon

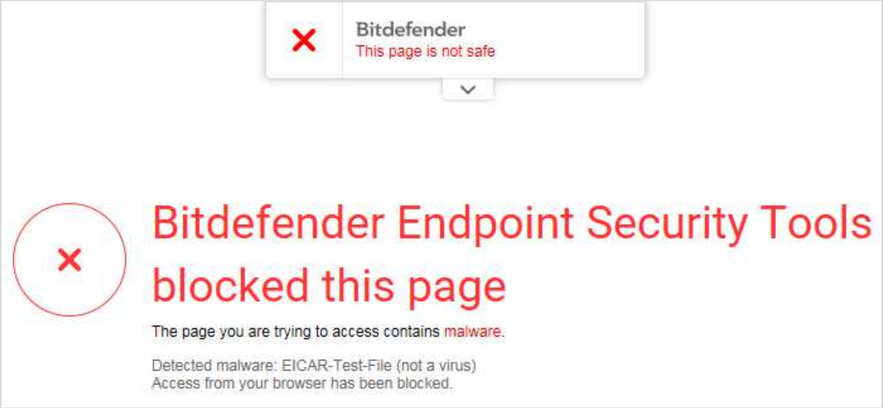
A System Tray icon is installed, which can be used to open the program or change the interface language.

### Unauthorised access

We could not find a means of disabling protection locally, even with an administrator account. Bitdefender inform us that administrators can configure this, with password protection, by means of a policy.

### Malware alerts

The following alert is shown in the browser when the EICAR test file is downloaded:



Bitdefender
This page is not safe

Bitdefender Endpoint Security Tools blocked this page

The page you are trying to access contains malware.

Detected malware: EICAR-Test-File (not a virus)
Access from your browser has been blocked.

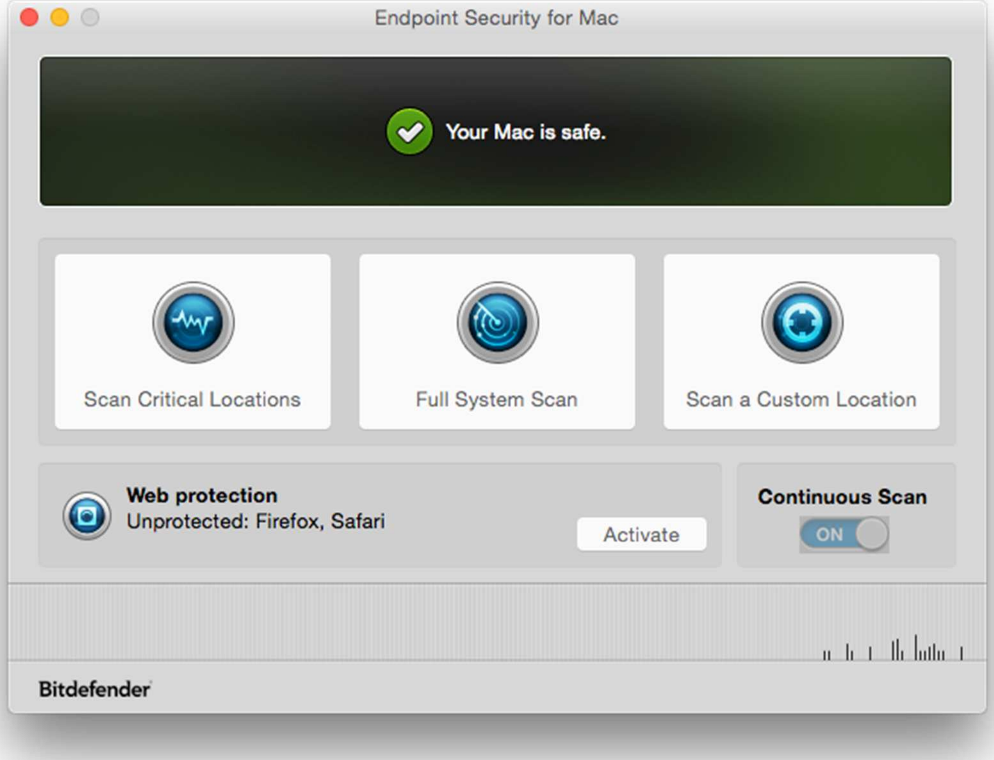
## Windows server protection software

This is identical to the Windows client protection software.

### Comment

The Windows client/server software provides a detailed overview of the status of all components, and allows users to run scans and updates, but not disable protection, which we find ideal. We have one very minor complaint: it is rather irritating that the window cannot be resized to show all components at once.

## Mac client protection software



### Installation

A .PKG installer file is downloaded from the console and run. The admin can change the location of the installation folder, but otherwise there are no choices to be made, and setup is completed with a few clicks.

### Main program window

This includes a status display and 3 scan buttons (Critical Locatons, Full, Custom). Updates can be run from the *Actions* menu in the Mac menu bar.

### System Tray icon

A System Tray icon is installed, from which the user can start the program or open the (minimal) configuration options.

### Unauthorised access

By default, it is not possible to deactivate protection, even with an administrator account.

### Malware alerts

In our test, the EICAR test file was blocked silently, i.e. we were not able to download the file, but no alert was shown.

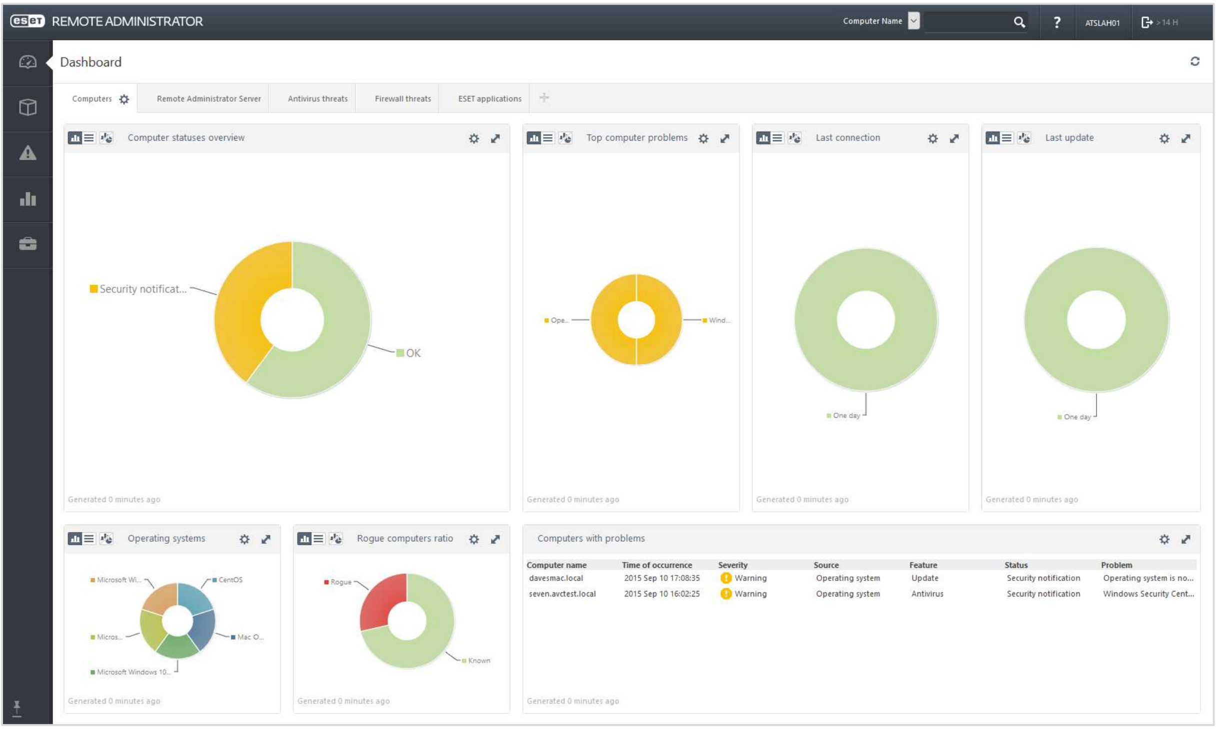
### Comment

The simple and familiar layout of the Mac client protection software shows users the status and allows them to run updates and scans, but not disable the protection, which we find ideal.

## Summary

We would recommend small businesses to have an IT professional set up the virtual appliance (very straightforward for an experienced professional) and provide basic training in everyday management. Non-expert administrators should then have no difficulty in carrying out day-to-day maintenance of the system. We found the console very easy to navigate, and the interface of the client software very appropriate. Excellent help features in the form of "welcome" pages in the console, and two comprehensive and well-produced manuals, provide all the necessary assistance.

# ESET Remote Administrator



| Computer name | Time of occurrence | Severity | Source | Feature | Status | Problem |
|---|---|---|---|---|---|---|
| davesmac.local | 2015 Sep 10 17:08:35 | Warning | Operating system | Update | Security notification | Operating system is no... |
| seven.avctest.local | 2015 Sep 10 16:02:25 | Warning | Operating system | Antivirus | Security notification | Windows Security Cent... |

Generated 0 minutes ago

## Introduction

For business users, ESET provides endpoint protection programs for Windows, Linux, Mac OS X, and Android. These could be installed and managed locally by very small businesses, or deployed and managed centrally using the ESET Remote Administrator console, which runs on the local area network. It can be installed on a Windows server, Linux server, or run as a virtual appliance under any one of a number of common virtualisation platforms. We used the virtual appliance for our test.

## Software versions reviewed

ESET Remote Administrator Version 6.2.11.0
ESET File Security for Windows 6.2.12007.0
ESET Endpoint Security for Windows 6.2.2021.0
ESET Endpoint Security for OS X 6.1.12.0

## Supported operating systems

Windows servers: Windows Server 2003, 2008/R2, 2012/R2; Windows Small Business Server 2003/R2, 2008, 2011
Windows clients: Windows XP, 7, 8, 8.1, 10
Mac OS clients: OS X 10.6, 10.7, 10.8, 10.10
Linux[5]
Android: please see feature list

[5] http://www.eset.com/int/business/endpoint-protection/linux-antivirus/

## Documentation

### Manuals

ESET provide a wide range of manuals for the product, including at least one document for each of the components (Remote Administrator console, License Administrator console, Windows file server, Windows client, Mac client etc.). All are detailed and produced to a very high standard; we particularly like the link on the front page of each manual which enables the user to download the latest version. To assist with our test, we used the ESET Remote Administrator 6 Installation Manual and User Guide, which is very comprehensive at 363 pages. It covers setting up the console on a Windows server or Linux server, or as a virtual appliance, along with all aspects of deploying and managing the endpoint protection software. It is easily accessible, thanks to bookmarks and a clickable contents page, well organised, clearly written and generously illustrated with screenshots that are annotated where appropriate.

### Knowledge base

An extensive searchable knowledge base is provided on ESET's website, covering a wide range of tasks. There are clear step-by-step instructions, also accompanied by annotated screenshots.

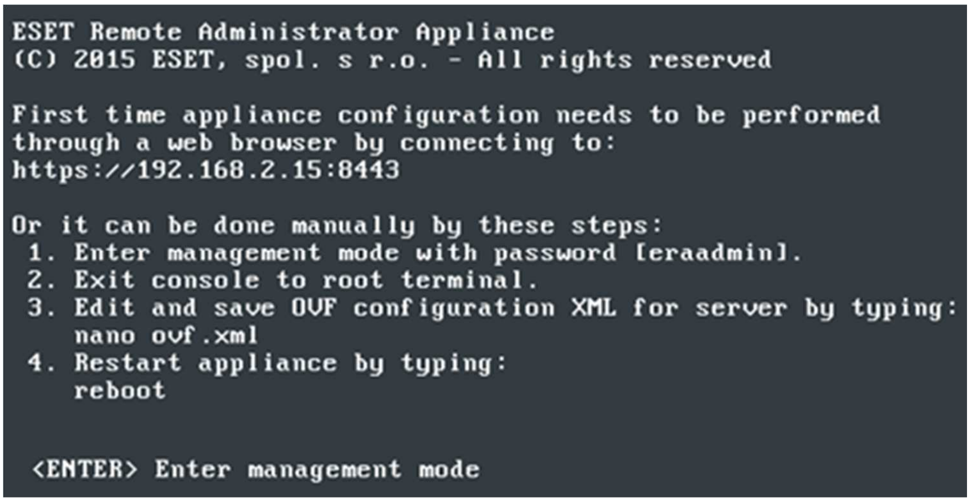
### Comment

We would describe the documentation for ESET Remote Administrator as outstanding.

## Management Console

### Installation and configuration

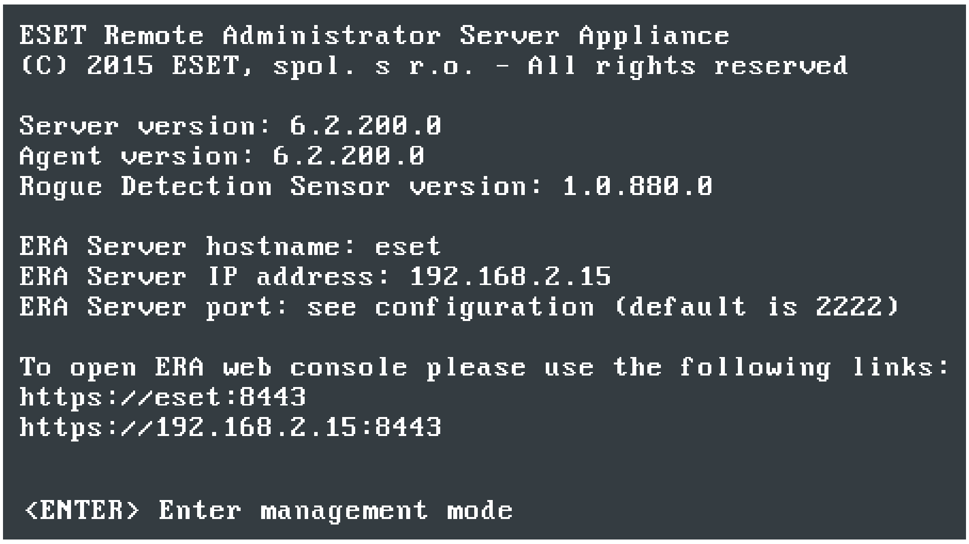
We use VMware Workstation to run the virtual appliance in our test. A virtual hard disk in .OVA format is downloaded from the ESET website and imported into VMware Workstation; this is a very straightforward procedure, and instructions for importing .OVA files are provided on the VMWare knowledge base.[6] The virtual machine thus created is then started, and it displays the URL to connect to in order to perform initial configuration:



```
ESET Remote Administrator Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved

First time appliance configuration needs to be performed
through a web browser by connecting to:
https://192.168.2.15:8443

Or it can be done manually by these steps:
 1. Enter management mode with password [eraadmin].
 2. Exit console to root terminal.
 3. Edit and save OVF configuration XML for server by typing:
    nano ovf.xml
 4. Restart appliance by typing:
    reboot


  <ENTER> Enter management mode
```

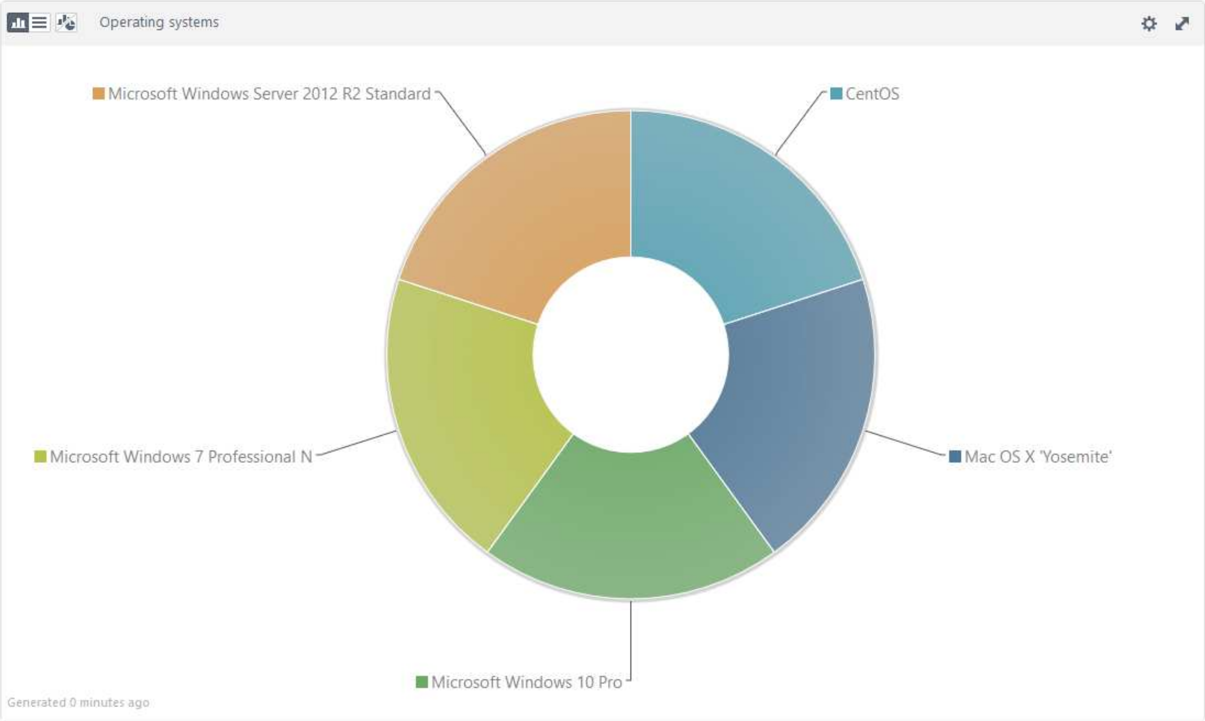
Having opened the URL in a browser, the admin configures the desired logon credentials, basic TCP/IP settings, and (optionally) Active Directory details if domain integration is required. Clicking *Submit* restarts the VM, which then displays the logon information for the console itself:

[6] http://pubs.vmware.com/workstation-10/index.jsp?topic=%2Fcom.vmware.ws.using.doc%2FGUID-DDCBE9C0-0EC9-4D09-8042-18436DA62F7A.html

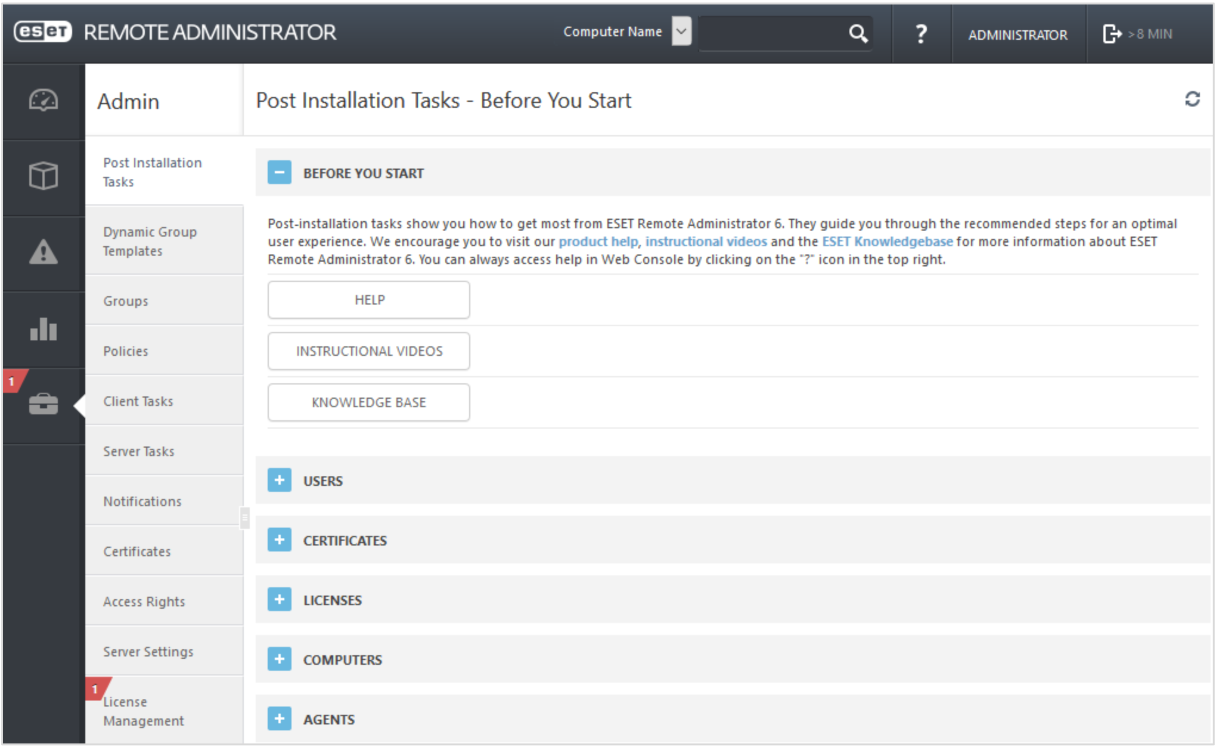


```
ESET Remote Administrator Server Appliance
(C) 2015 ESET, spol. s r.o. - All rights reserved

Server version: 6.2.200.0
Agent version: 6.2.200.0
Rogue Detection Sensor version: 1.0.880.0

ERA Server hostname: eset
ERA Server IP address: 192.168.2.15
ERA Server port: see configuration (default is 2222)

To open ERA web console please use the following links:
https://eset:8443
https://192.168.2.15:8443


 <ENTER> Enter management mode
```

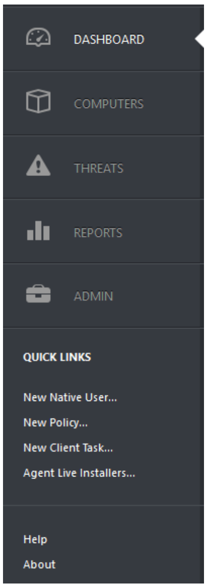
The admin can then log on to the console with a web browser. We note that virtual appliance is shown in the dashboard (Shown as *CentOS* in the *Operating Systems* panel shown below), and can be monitored and managed along with Windows and Mac computers.



When the admin first logs on to the console, two alerts are shown; the first points to the *Post Installation Tasks* page, which provides a quick-start guide to using the console. The second relates to licence management, and prompts the admin to enter the licence key.



Post-installation tasks show you how to get most from ESET Remote Administrator 6. They guide you through the recommended steps for an optimal user experience. We encourage you to visit our product help, instructional videos and the ESET Knowledgebase for more information about ESET Remote Administrator 6. You can always access help in Web Console by clicking on the "?" icon in the top right.



## Layout

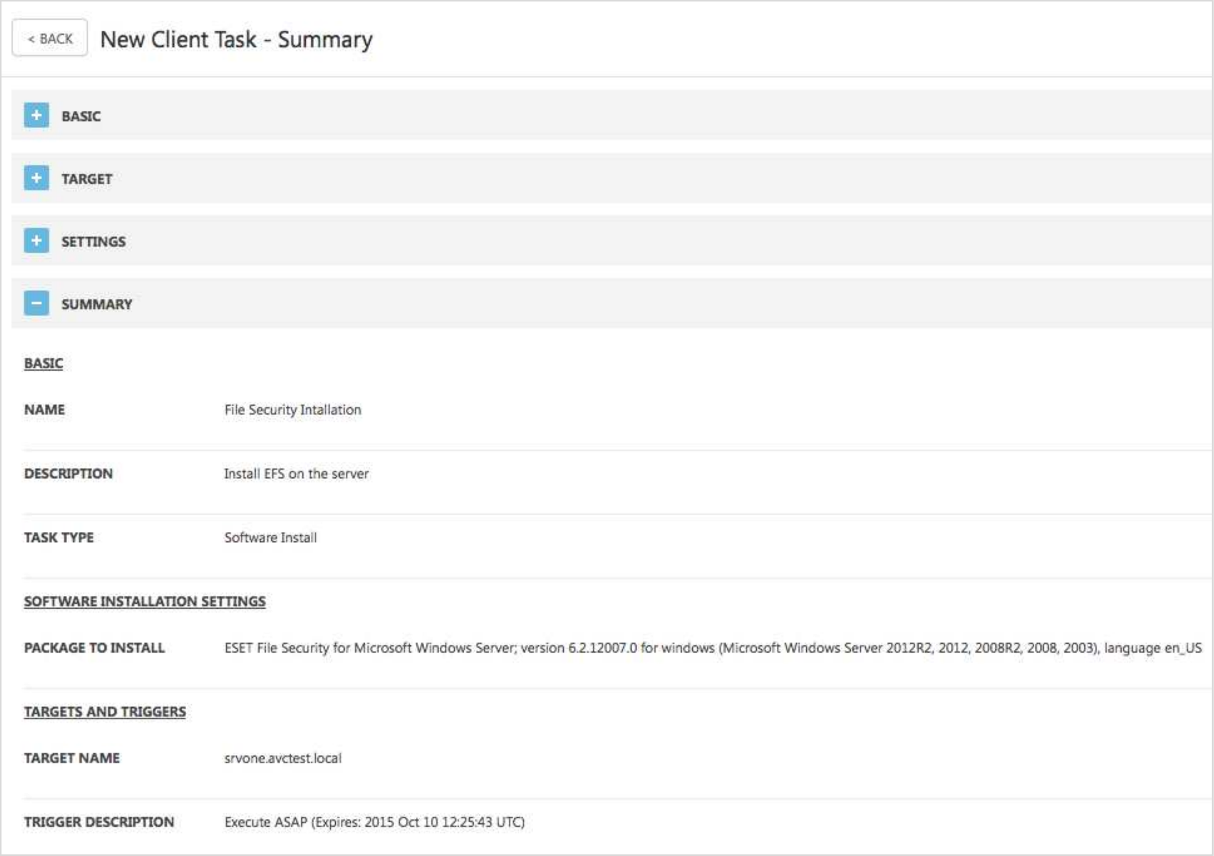
The menu panel on the left-hand side of the console, seen in the screenshot above, allows the admin to access the five main functional areas of the console, namely *Dashboard*, *Computers*, *Threats*, *Reports,* and *Admin*, the latter including the *Post Installation Tasks* page. Moving the mouse over this panel expands it, displaying the features' names and some additional links, as shown on the left. It is possible to pin the panel closed, preventing it from expanding on mouse-over; we would like to have the option to pin it open, so that the names and links are always displayed, but unfortunately this is not possible.

## Preparing devices for deployment

We did not make any preparations on client or server systems before deployment.

## Deploying the endpoint protection software

The first stage of deploying the endpoint protection software is to install the ERA agent – please see the respective sections on Windows and Mac clients for details. After this, the endpoint client itself can be deployed remotely from the console. The admin goes to the *Computers* page, selects the computer(s) to be installed, selects *New task…* from *Tasks* menu. This opens the *New Task* page, where the admin fills in details of the computer(s) and product to be installed. The admin can deploy an individual installation package to any number of computers at once, but separate tasks have to be created respectively for Windows servers, Windows clients and Mac clients. A summary of the task details entered is shown at the end:



BASIC

| | |
|---|---|
| NAME | File Security Intallation |
| DESCRIPTION | Install EFS on the server |
| TASK TYPE | Software Install |

SOFTWARE INSTALLATION SETTINGS

| | |
|---|---|
| PACKAGE TO INSTALL | ESET File Security for Microsoft Windows Server; version 6.2.12007.0 for windows (Microsoft Windows Server 2012R2, 2012, 2008R2, 2008, 2003), language en_US |

TARGETS AND TRIGGERS

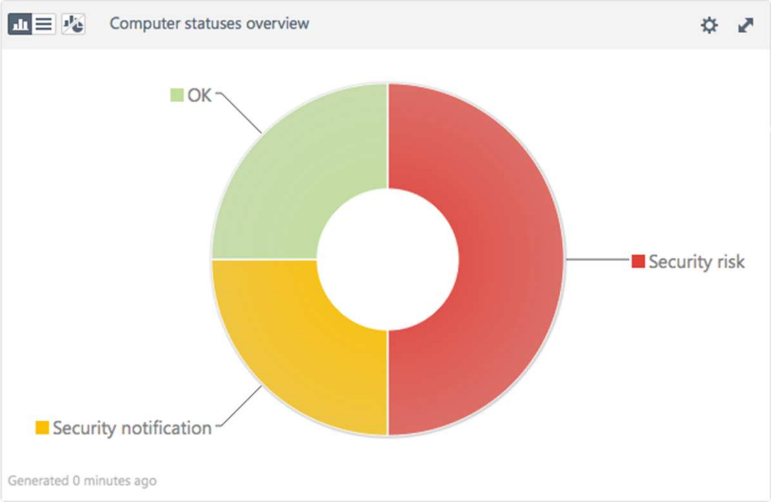
| | |
|---|---|
| TARGET NAME | srvone.avctest.local |
| TRIGGER DESCRIPTION | Execute ASAP (Expires: 2015 Oct 10 12:25:43 UTC) |

In our test, we found that the software was installed on the target computers very quickly (in about a minute) after we had clicked *Finish* to run the task. We note that it is necessary to activate the protection software after installation; this can be done locally or via the console, by creating a Task in just the same way as for the deployment.

## Monitoring the network

### *Status*

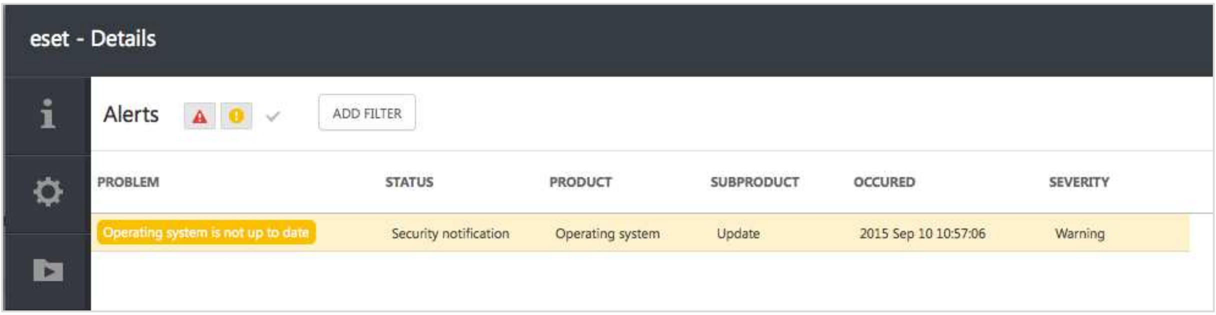
The *Computer statuses overview* panel of the dashboard shows security status of the network in the form of a pie chart, with each segment showing the proportion of all devices in a particular state:



Other panels of the *Dashboard* provide further status information, such as *Top computer problems, Rogue computers ratio, Computers with problems.*

### *Warnings*

As shown in the screenshot above, there are two types of warning: *Security notification* (minor alert, e.g. operating system not up to date), and *Security risk* (more serious alert, e.g. protection disabled). The respective traffic-light colours are used to indicate the two alert states and the OK state (the same colouring is used to show warnings on the *Computers* page as well). Clicking on one of the coloured areas displays the menu below; clicking on *Detailed information* shows a list of affected computers, from which details of the specific problem can be seen:



eset - Details

Alerts ADD FILTER

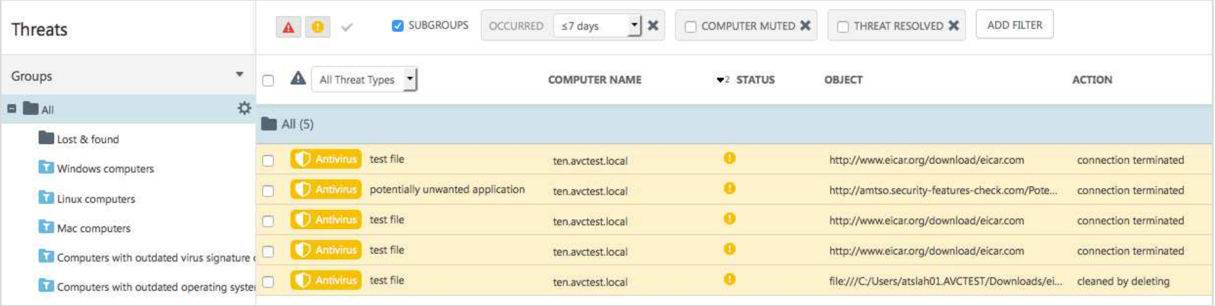
| PROBLEM | STATUS | PRODUCT | SUBPRODUCT | OCCURED | SEVERITY |
|---|---|---|---|---|---|
| Operating system is not up to date | Security notification | Operating system | Update | 2015 Sep 10 10:57:06 | Warning |

### *Rectifying problems*

In some cases, e.g. malware signatures being out of date, a problem can be solved from the console by running the appropriate task, such as an update or reboot. At the time of writing, mid-September 2015, there was no task for reactivating disabled protection, although we understand from ESET that this is under development.

### *Malware alerts*

Malware detections can be seen very easily by clicking the *Threats* button in the left-hand menu pane of the console. This displays details[7] of malicious software found:



Threats

Groups

- All
  - Lost & found
  - Windows computers
  - Linux computers
  - Mac computers
  - Computers with outdated virus signature (
  - Computers with outdated operating syste

☑ SUBGROUPS OCCURRED ≤7 days ✖ □ COMPUTER MUTED ✖ □ THREAT RESOLVED ✖ ADD FILTER

All (5)

| □ | All Threat Types | COMPUTER NAME | STATUS | OBJECT | ACTION |
|---|---|---|---|---|---|
| □ | Antivirus test file | ten.avctest.local | ● | http://www.eicar.org/download/eicar.com | connection terminated |
| □ | Antivirus potentially unwanted application | ten.avctest.local | ● | http://amtso.security-features-check.com/Pote... | connection terminated |
| □ | Antivirus test file | ten.avctest.local | ● | http://www.eicar.org/download/eicar.com | connection terminated |
| □ | Antivirus test file | ten.avctest.local | ● | http://www.eicar.org/download/eicar.com | connection terminated |
| □ | Antivirus test file | ten.avctest.local | ● | file:///C:/Users/atslah01.AVCTEST/Downloads/ei... | cleaned by deleting |

### *Program version*

This is shown on the *Computers* page.

## Managing the network

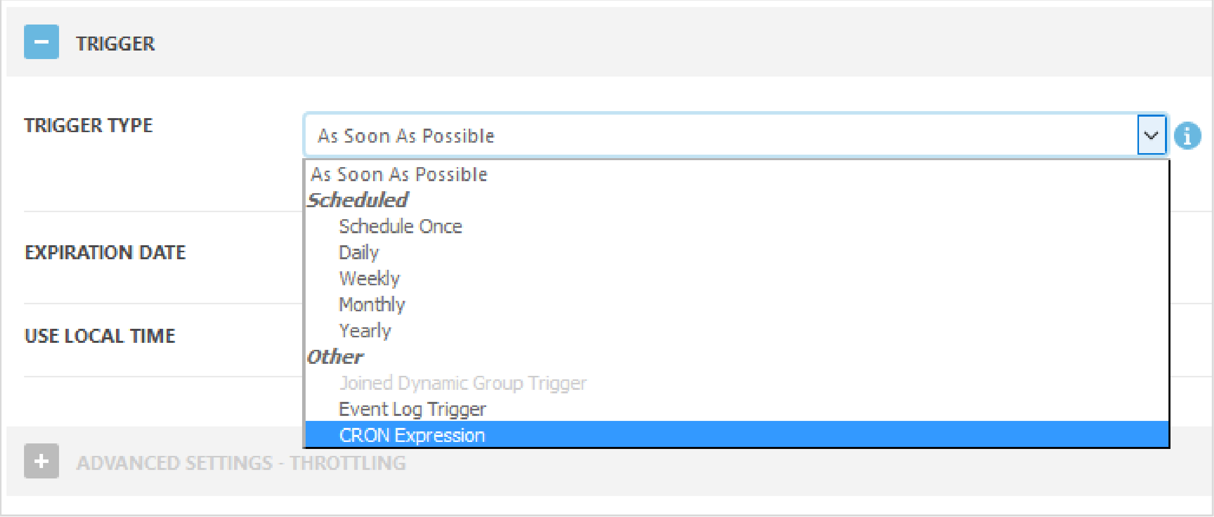
### *Scanning*

Scans can be run by selecting the relevant computer(s) from the *Computers* page, and clicking *Scan* in the *Tasks* menu, which runs a standard scan. Alternatively, the admin can click *New Task…* and choose *In-Depth*, *Smart* or *Custom Scan*.

[7] Please note that we have customised the order of the columns to show the most important items in the screenshot.

### *Scheduling Scans*

To set a scheduled scan, the admin creates a new scan task, and then selects one of the *Scheduled* options under *Trigger*:



### *Updates*

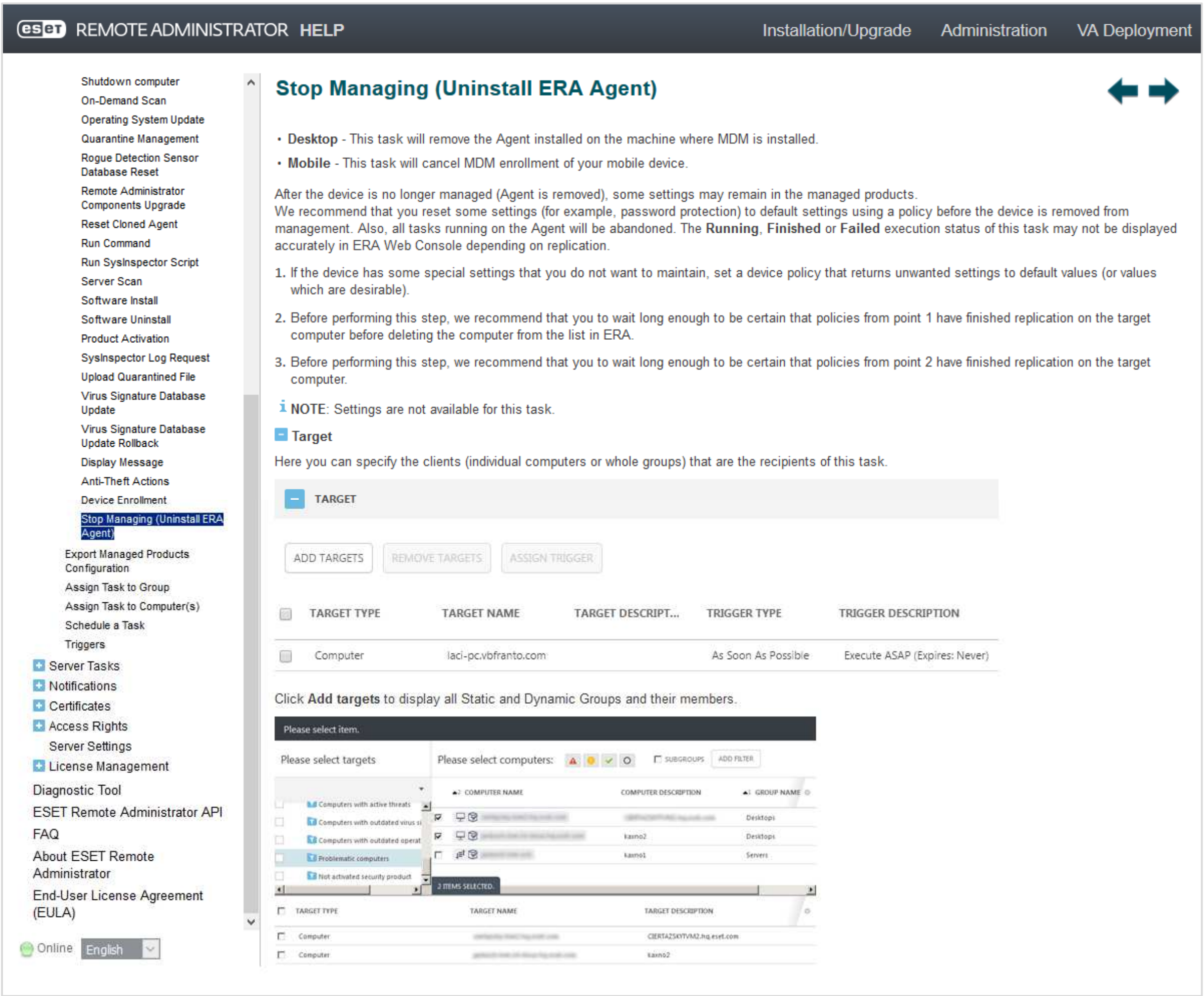
To update malware definitions, the admin selects computers from the *Computers* page, then clicks *Update Virus DB* in the *Tasks* menu. The update then runs with no further interaction required.

### *Removing devices from the console*

A computer can be removed from the console by uninstalling the ERA Agent. This is done by running a Task, selecting *ESET Remote Administrator* under *Task Category,* and *Stop Managing (Uninstall ERA Agent)* under *Task*.

### Integrated help feature

This is context-sensitive, i.e. opens at the correct section for the console page currently being viewed. A comprehensive list of tasks is shown in a left-hand panel, with detailed, well-illustrated instructions in the main panel:



Shutdown computer
On-Demand Scan
Operating System Update
Quarantine Management
Rogue Detection Sensor Database Reset
Remote Administrator Components Upgrade
Reset Cloned Agent
Run Command
Run SysInspector Script
Server Scan
Software Install
Software Uninstall
Product Activation
SysInspector Log Request
Upload Quarantined File
Virus Signature Database Update
Virus Signature Database Update Rollback
Display Message
Anti-Theft Actions
Device Enrollment
Stop Managing (Uninstall ERA Agent)
Export Managed Products Configuration
Assign Task to Group
Assign Task to Computer(s)
Schedule a Task
Triggers
Server Tasks
Notifications
Certificates
Access Rights
Server Settings
License Management
Diagnostic Tool
ESET Remote Administrator API
FAQ
About ESET Remote Administrator
End-User License Agreement (EULA)

Online English

**Stop Managing (Uninstall ERA Agent)**

- **Desktop** - This task will remove the Agent installed on the machine where MDM is installed.
- **Mobile** - This task will cancel MDM enrollment of your mobile device.

After the device is no longer managed (Agent is removed), some settings may remain in the managed products. We recommend that you reset some settings (for example, password protection) to default settings using a policy before the device is removed from management. Also, all tasks running on the Agent will be abandoned. The **Running**, **Finished** or **Failed** execution status of this task may not be displayed accurately in ERA Web Console depending on replication.

1. If the device has some special settings that you do not want to maintain, set a device policy that returns unwanted settings to default values (or values which are desirable).
2. Before performing this step, we recommend that you to wait long enough to be certain that policies from point 1 have finished replication on the target computer before deleting the computer from the list in ERA.
3. Before performing this step, we recommend that you to wait long enough to be certain that policies from point 2 have finished replication on the target computer.

NOTE: Settings are not available for this task.

**Target**

Here you can specify the clients (individual computers or whole groups) that are the recipients of this task.

TARGET

ADD TARGETS | REMOVE TARGETS | ASSIGN TRIGGER

| □ | TARGET TYPE | TARGET NAME | TARGET DESCRIPT... | TRIGGER TYPE | TRIGGER DESCRIPTION |
|---|---|---|---|---|---|
| □ | Computer | laci-pc.vbfranto.com | | As Soon As Possible | Execute ASAP (Expires: Never) |

Click **Add targets** to display all Static and Dynamic Groups and their members.

Please select item.

Please select targets

- □ Computers with active threats
- □ Computers with outdated virus si
- □ Computers with outdated operat
- □ Problematic computers
- □ Not activated security product

Please select computers: □ SUBGROUPS ADD FILTER

| | COMPUTER NAME | COMPUTER DESCRIPTION | GROUP NAME |
|---|---|---|---|
| ☑ | [redacted] | [redacted] | Desktops |
| ☑ | [redacted] | kaxno2 | Desktops |
| □ | [redacted] | kaxno1 | Servers |

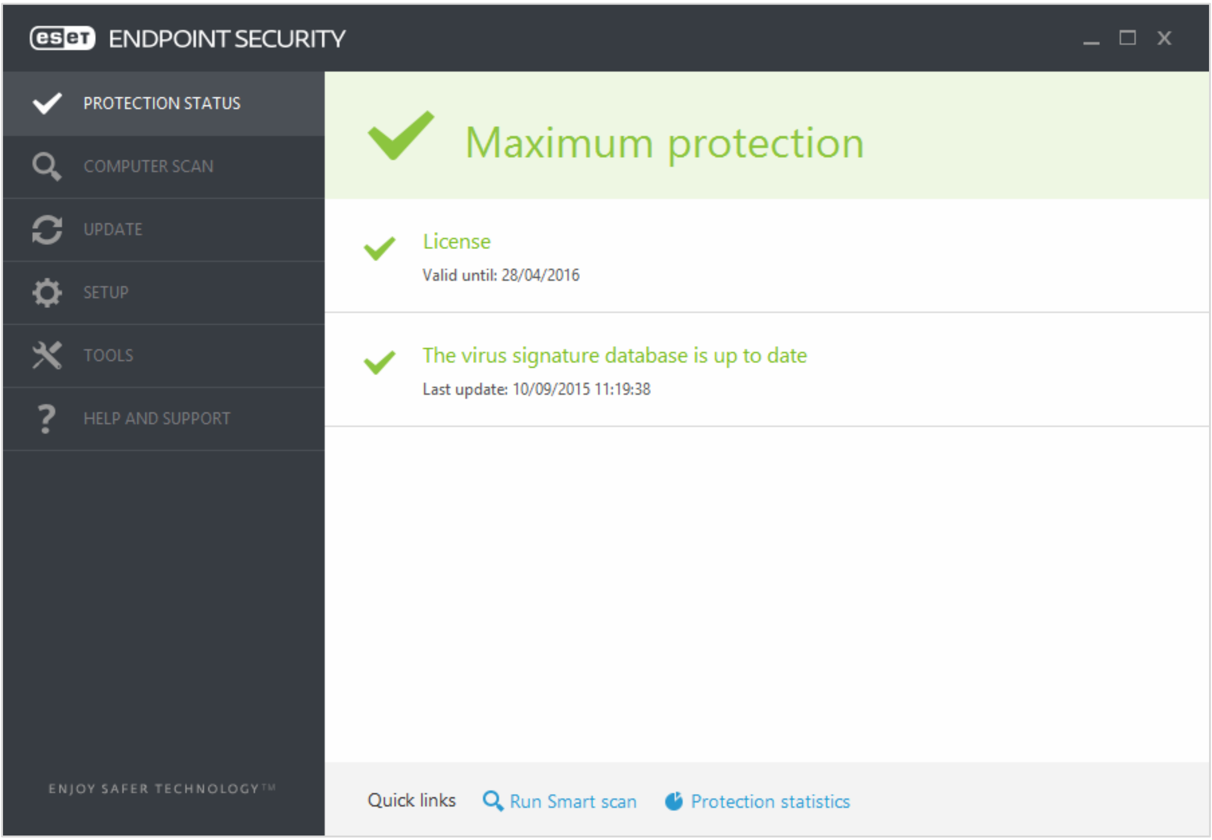
2 ITEMS SELECTED.

| □ | TARGET TYPE | TARGET NAME | TARGET DESCRIPTION |
|---|---|---|---|
| □ | Computer | [redacted] | CIERTA2SKYTVM2.hq.eset.com |
| □ | Computer | [redacted] | kaxno2 |

## Comment

For an experienced Windows administrator, ESET Remote Administrator is very straightforward to set up, with no specialist Linux knowledge required. With a little help from the excellent documentation and help features, we quickly found our way around the console and its functions; we liked the customisable Dashboard page and the very consistent layout and functionality. We would suggest that any small business using the product should have an IT professional set up the console and provide a little basic training, after which we feel that non-expert administrators should be able to use it without any difficulty.

## Windows client protection software



Maximum protection

License
Valid until: 28/04/2016

The virus signature database is up to date
Last update: 10/09/2015 11:19:38

### Installation

We deployed the ERA Agent by running the .MSI installer file locally on the client computer. The admin has to enter the management server's hostname or IP address and specify the port (this has already entered and can normally be left as it is) and administrator credentials. When the agent setup wizard has completed, the computer can be seen in the console, and the endpoint protection itself can then be deployed remotely, as described above.

### Main program window

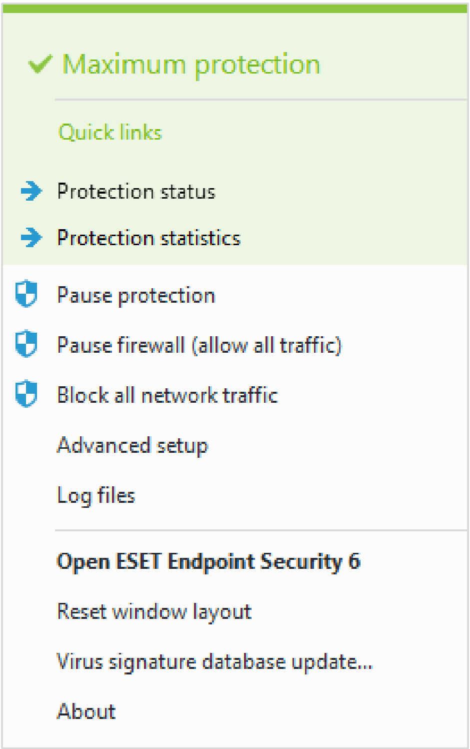
This includes a status display, licence information, and links to scans, update and help.

### Windows Security Center/Windows Defender

ESET Endpoint Security registers as antivirus, antispyware and firewall. Under Windows 7, Windows Defender is not disabled.

### System Tray icon

A system tray icon is installed, which displays the following menu if right-clicked:

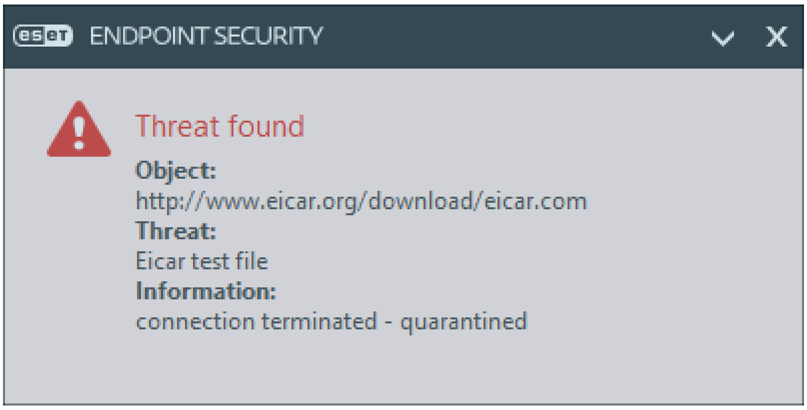


### Unauthorised access

When logged on with a non-administrator account, we were not able to deactivate the protection, as a Windows UAC dialog demands administrator credentials.

### Malware alerts

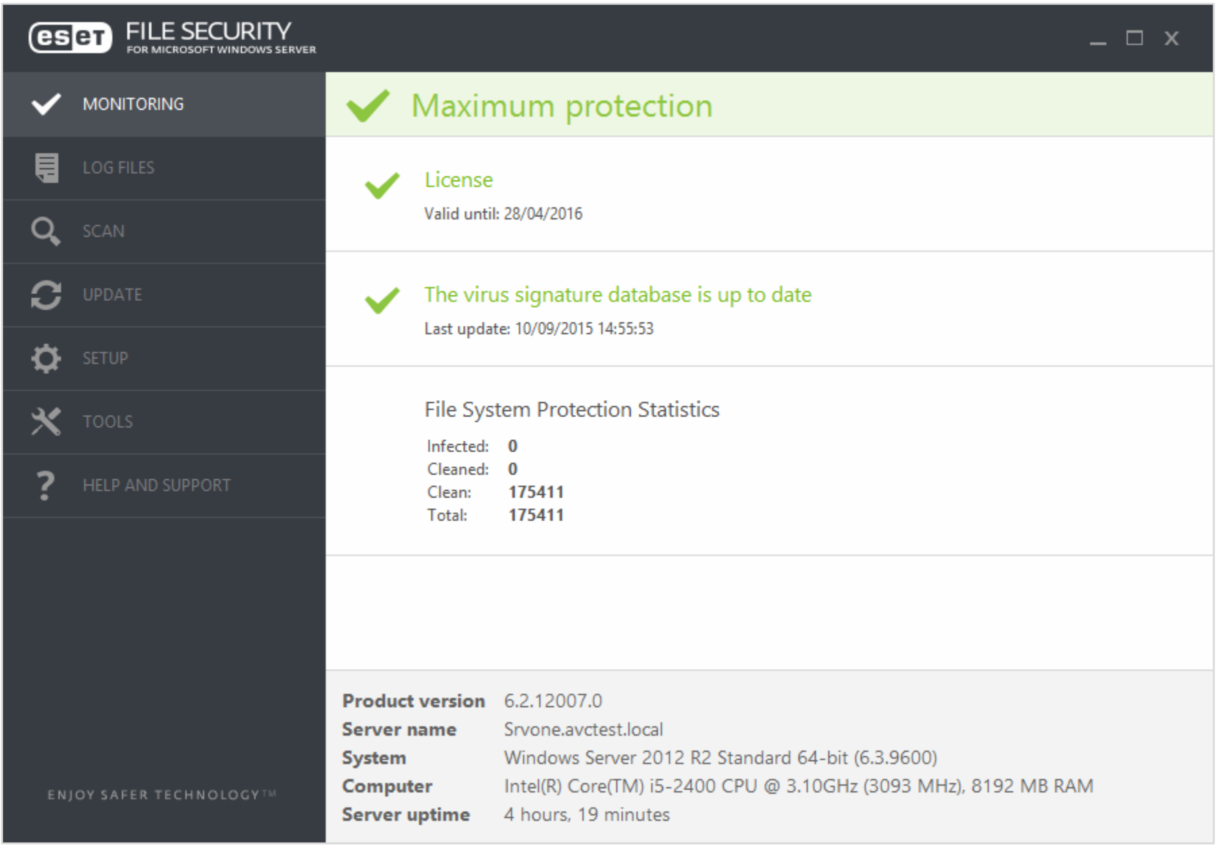
The following alert is shown when the EICAR test file is downloaded:



Threat found

**Object:**
http://www.eicar.org/download/eicar.com
**Threat:**
Eicar test file
**Information:**
connection terminated - quarantined

## Windows server protection software



✓ Maximum protection

✓ License
Valid until: 28/04/2016

✓ The virus signature database is up to date
Last update: 10/09/2015 14:55:53

File System Protection Statistics

| | |
|---|---|
| Infected: | 0 |
| Cleaned: | 0 |
| Clean: | 175411 |
| Total: | 175411 |

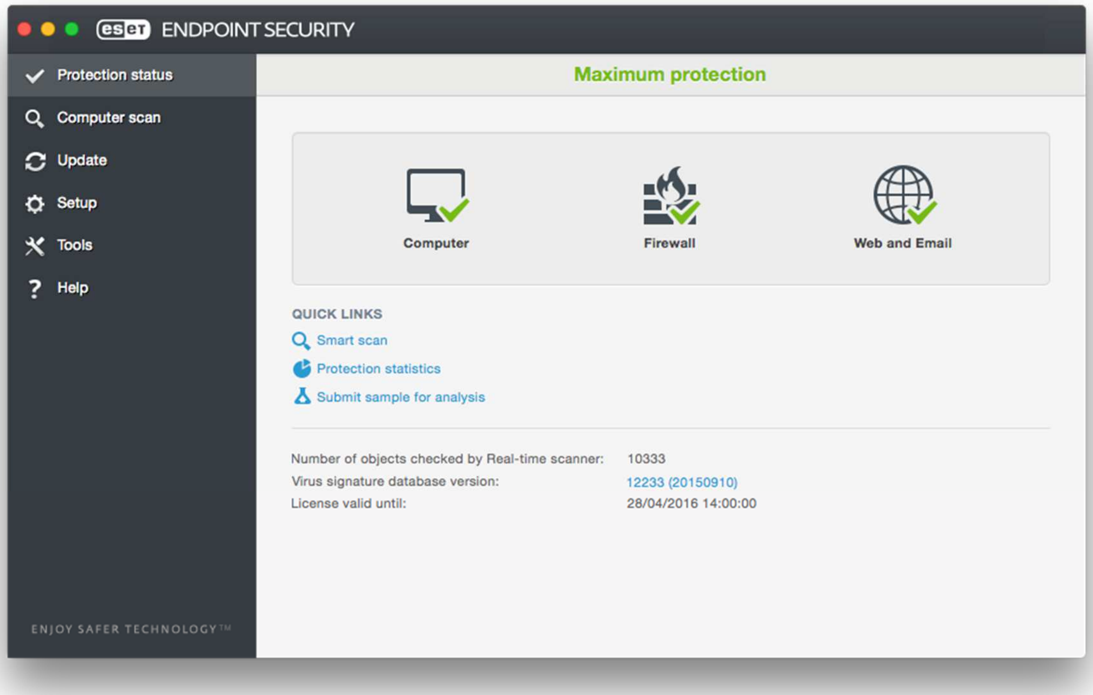
| | |
|---|---|
| **Product version** | 6.2.12007.0 |
| **Server name** | Srvone.avctest.local |
| **System** | Windows Server 2012 R2 Standard 64-bit (6.3.9600) |
| **Computer** | Intel(R) Core(TM) i5-2400 CPU @ 3.10GHz (3093 MHz), 8192 MB RAM |
| **Server uptime** | 4 hours, 19 minutes |

The installation of ESET File Security is equivalent to that of Endpoint Security. The user interface is also extremely similar to that of the client software, the differences being that the status page (*Monitoring*) displays additional system information, and there is an additional button in the menu panel, *Log Files*.

### Comment

We feel the Windows protection software is exceptionally well designed, with important information and functions easily accessible, but unauthorised access prevented. The consistency of design between server and client versions is helpful, and we note that the interface would be very finger-friendly if used with a touchscreen.

## Mac client protection software



Number of objects checked by Real-time scanner: 10333
Virus signature database version: 12233 (20150910)
License valid until: 28/04/2016 14:00:00

### Installation

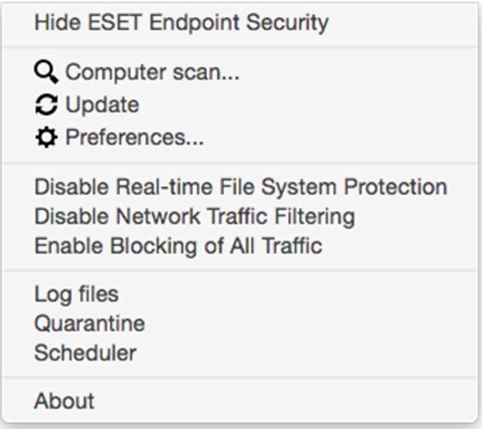
We deployed ESET Endpoint Security for OS X in the same way as the Windows protection software, i.e. by manually installing the agent and then pushing the endpoint protection client from the console. It should be noted that the agent installer comes in the form of a .TAR.GZ file, containing an .SH file which has to be extracted and then run using the OS X Terminal. As Mac OS X is Unix-based, this procedure would be familiar to e.g. Linux users. Fortunately, ESET provide illustrated instructions in their knowledge base for Windows admins who are not familiar with such things.[8]

### Main program window

This has a status display, subscription information, and links to scans, updates and help.

### System Tray icon

A System Tray icon is installed, which shows the following menu:


Hide ESET Endpoint Security
Computer scan...
Update
Preferences...
Disable Real-time File System Protection
Disable Network Traffic Filtering
Enable Blocking of All Traffic
Log files
Quarantine
Scheduler
About

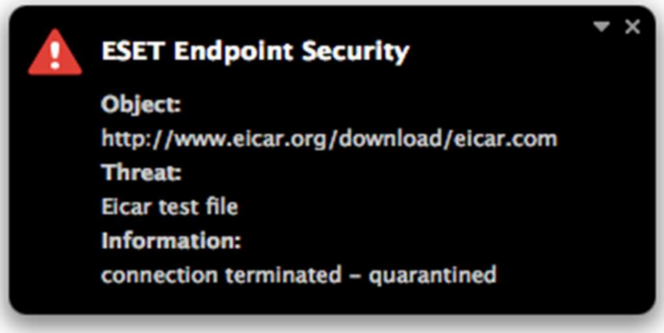
[8] http://support.eset.com/kb3696/?viewlocale=en_US

## Unauthorised access

When a standard user is logged on, the controls for disabling the protection are either hidden or deactivated, preventing the user from deactivating the program.

## Malware alerts

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



ESET Endpoint Security

Object:
http://www.eicar.org/download/eicar.com
Threat:
Eicar test file
Information:
connection terminated – quarantined

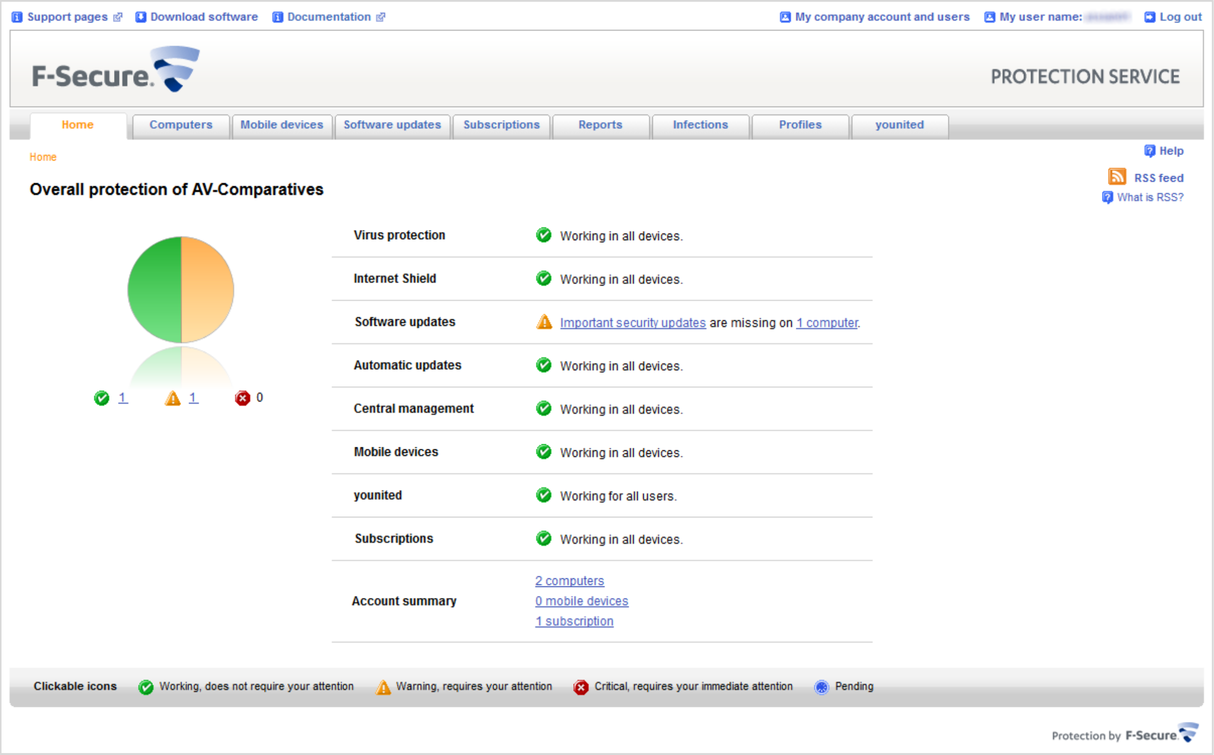
## Comment

Like its Windows counterparts, ESET Endpoint Security for OS X provides the user with useful status information, plus update and scan controls, but prevents unauthorised access to the settings. We feel the consistency of design across the different platforms will simplify life for the administrator.

## Summary

The ESET Remote Administrator console has comprehensive functionality and could be used to manage enterprise-level networks, but is nonetheless very straightforward to set up and find one's way around. With a little initial help from an IT consultant, it could easily be used by a small business without permanent IT staff. Two outstanding features of the product are its comprehensive, clear and well-illustrated documentation/help facilities, and the neatly designed and easy-to-use endpoint protection software. There is a high degree of consistency among the versions for the different platforms, and also between the client software and the console; configuration pages in client settings are mirrored in their console counterparts, for example.

# F-Secure Protection Service for Business



Support pages | Download software | Documentation | My company account and users | My user name: [redacted] | Log out

F-Secure. PROTECTION SERVICE

Home | Computers | Mobile devices | Software updates | Subscriptions | Reports | Infections | Profiles | younited

Home

Help
RSS feed
What is RSS?

Overall protection of AV-Comparatives

✓ 1 ⚠ 1 ✗ 0

| | |
|---|---|
| Virus protection | ✓ Working in all devices. |
| Internet Shield | ✓ Working in all devices. |
| Software updates | ⚠ Important security updates are missing on 1 computer. |
| Automatic updates | ✓ Working in all devices. |
| Central management | ✓ Working in all devices. |
| Mobile devices | ✓ Working in all devices. |
| younited | ✓ Working for all users. |
| Subscriptions | ✓ Working in all devices. |
| Account summary | 2 computers<br>0 mobile devices<br>1 subscription |

Clickable icons ✓ Working, does not require your attention ⚠ Warning, requires your attention ✗ Critical, requires your immediate attention ● Pending

Protection by F-Secure

## Introduction

F-Secure produce a wide range of products for both large and small businesses, including endpoint security for Windows, Mac OS X, Linux, and various mobile platforms, along with antivirus for file servers, mail servers and gateways. This review covers F-Secure Protection Service for Business, which uses a web-based console to manage security software for client devices, and is suitable for small businesses.

## Software versions reviewed

PSB Server Security for Windows 11.00 build 236
PSB Workstation Security for Windows 10.6
PSB Workstation Security for Mac 15465
PSB Console as at 30th August 2015

## Supported operating systems

Windows clients: Windows XP (32-bit), Vista, 7, 8, 8.1, 10
Windows servers: Windows Server 2003/R2, 2008/R2, 2012, 2012 Essentials;
Small Business Server 2003/R2, 2008, 2011, 2011 Essentials
Mac OS X clients: Mac OS X 10.6, 10.7, 10.8, 10.9, 10.10 [10.11 support planned[9]]
Linux[10]
Android/iOS: please see feature list

[9] A new Mac client version is to be released in Q4 2015, with support for OS X 10.11
[10] https://www.f-secure.com/en/web/business_global/downloads/protection-service-for-business/latest

## Documentation

### Manuals

F-Secure provide two manuals for the product, a 24-page Getting Started Guide, and a 58-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.

### Knowledge base

F-Secure also have a knowledge base on their website, which provides answers to common questions.

### Comment

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

## Management Console

### Installation and configuration

The console is cloud-based and so requires no installation; the admin simply goes to the URL, creates an account, and logs in.

### Layout

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.

### Preparing devices for deployment

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

### Deploying the endpoint protection software

The endpoint protection software can be installed by downloading the setup file from the console; the admin clicks *Download the software* in the top left-hand corner of the console. Alternatively, the Computers tab of 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.

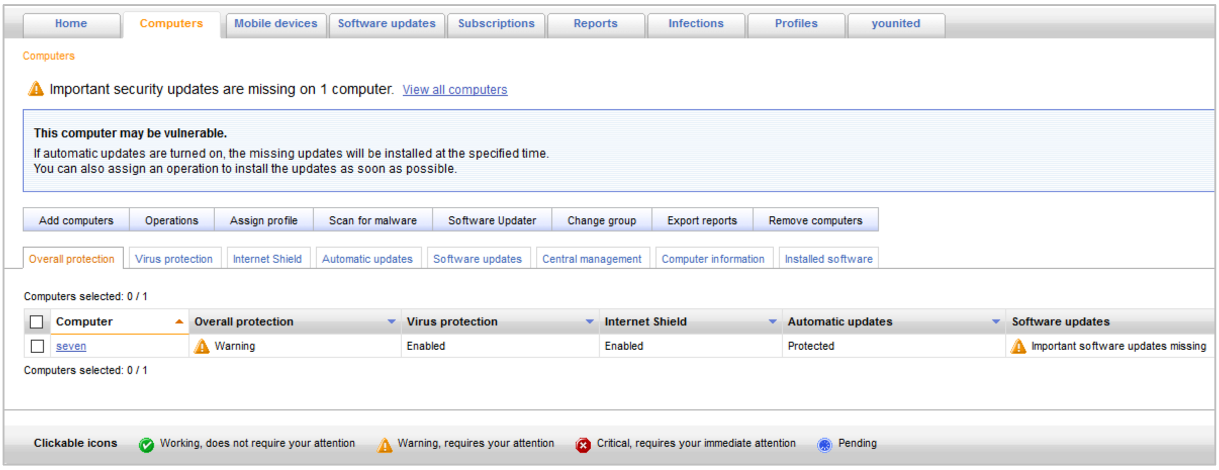
## Monitoring the network

### Status

The home page shows the overall status of devices on the network, as in the main screenshot above. a list of components within the endpoint protection software is displayed; if all is well on all devices, the status is shown as “Working in all devices”.

### Warnings

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 shows the administrator which computers are affected:



Important security updates are missing on 1 computer. View all computers

**This computer may be vulnerable.**

If automatic updates are turned on, the missing updates will be installed at the specified time.
You can also assign an operation to install the updates as soon as possible.

Computers selected: 0 / 1

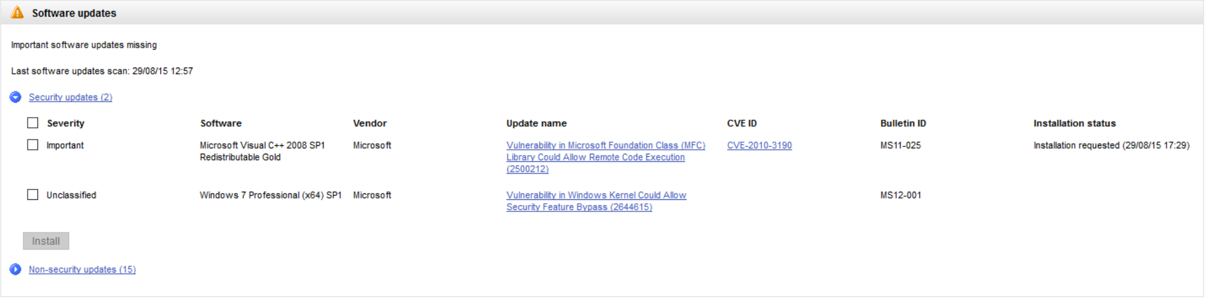
| □ | Computer | Overall protection | Virus protection | Internet Shield | Automatic updates | Software updates |
|---|---|---|---|---|---|---|
| □ | seven | ⚠ Warning | Enabled | Enabled | Protected | ⚠ Important software updates missing |

Computers selected: 0 / 1

Clickable icons ✓ Working, does not require your attention ⚠ Warning, requires your attention ✕ Critical, requires your immediate attention ● Pending

### Rectifying problems

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



⚠ Software updates

Important software updates missing

Last software updates scan: 29/08/15 12:57

Security updates (2)

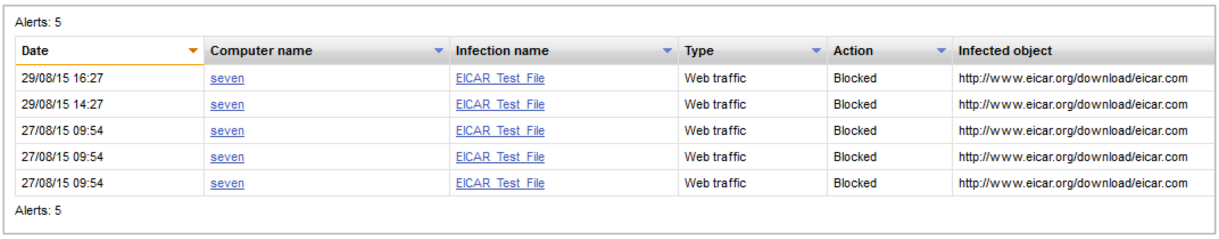
| □ Severity | Software | Vendor | Update name | CVE ID | Bulletin ID | Installation status |
|---|---|---|---|---|---|---|
| □ Important | Microsoft Visual C++ 2008 SP1 Redistributable Gold | Microsoft | Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execution (2500212) | CVE-2010-3190 | MS11-025 | Installation requested (29/08/15 17:29) |
| □ Unclassified | Windows 7 Professional (x64) SP1 | Microsoft | Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615) | | MS12-001 | |

Non-security updates (15)

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).

### Malware alerts

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.



Alerts: 5

| Date | Computer name | Infection name | Type | Action | Infected object |
|---|---|---|---|---|---|
| 29/08/15 16:27 | seven | EICAR_Test_File | Web traffic | Blocked | http://www.eicar.org/download/eicar.com |
| 29/08/15 14:27 | seven | EICAR_Test_File | Web traffic | Blocked | http://www.eicar.org/download/eicar.com |
| 27/08/15 09:54 | seven | EICAR_Test_File | Web traffic | Blocked | http://www.eicar.org/download/eicar.com |
| 27/08/15 09:54 | seven | EICAR_Test_File | Web traffic | Blocked | http://www.eicar.org/download/eicar.com |
| 27/08/15 09:54 | seven | EICAR_Test_File | Web traffic | Blocked | http://www.eicar.org/download/eicar.com |

Alerts: 5

### *Program version*

The software version installed can be found by clicking the *Computers* tab, *Installed Software* sub-tab.

## Managing the network

### *Scanning*

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.

### *Scheduling Scans*

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.

### *Updates*

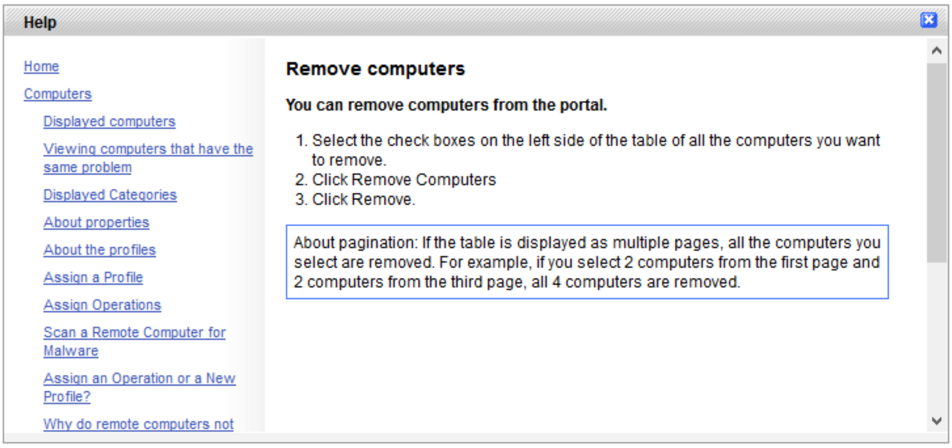
Updates are run automatically at pre-configured intervals. Manual updates can be run from the local client software on each computer.

### *Removing devices from the console*

This can be done by going to the *Computers Tab, Remove Computers* sub-tab, selecting the relevant device and clicking *Remove*.

## Integrated help feature

Clicking *Help* in the top right-hand corner of the console opens the integrated help box, which provides simple text instructions for common tasks:



Help
Home
Computers
Displayed computers
Viewing computers that have the same problem
Displayed Categories
About properties
About the profiles
Assign a Profile
Assign Operations
Scan a Remote Computer for Malware
Assign an Operation or a New Profile?
Why do remote computers not

**Remove computers**

**You can remove computers from the portal.**

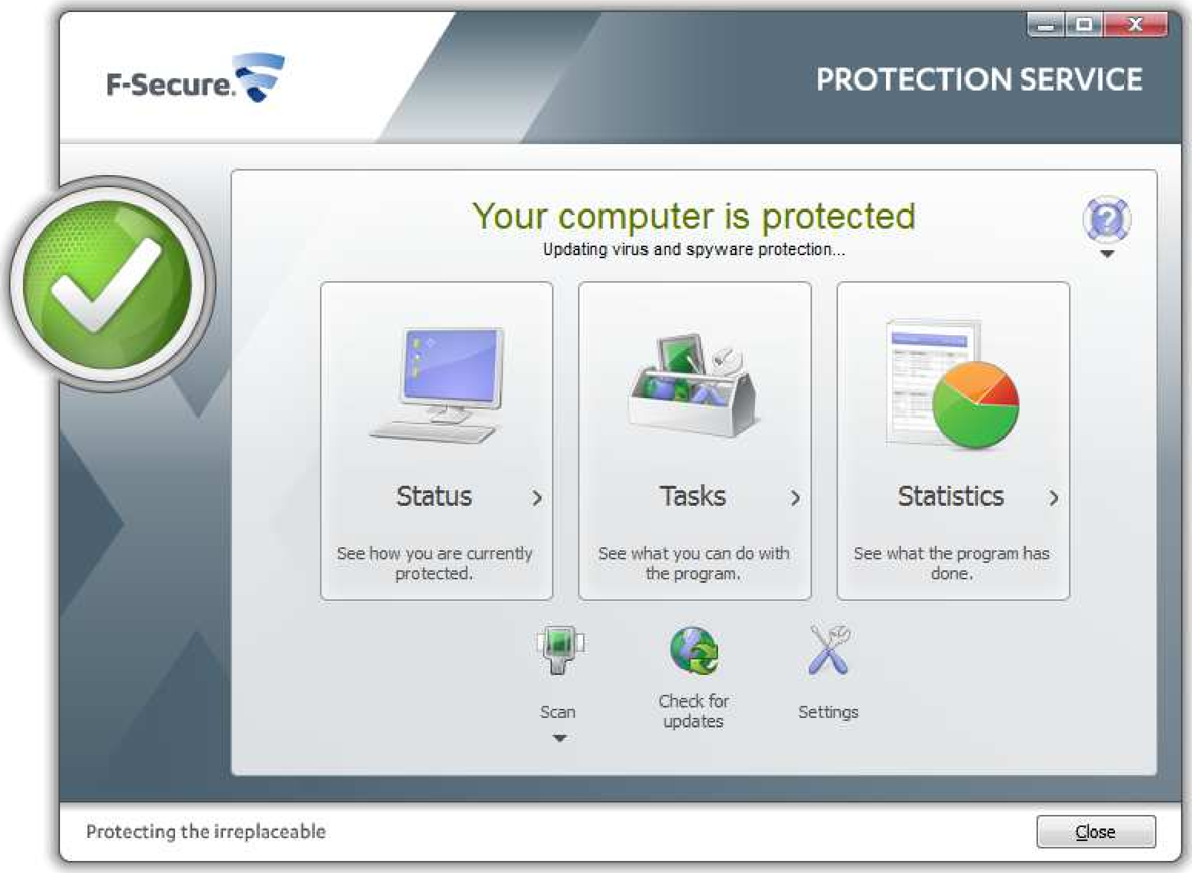
1. Select the check boxes on the left side of the table of all the computers you want to remove.
2. Click Remove Computers
3. Click Remove.

About pagination: If the table is displayed as multiple pages, all the computers you select are removed. For example, if you select 2 computers from the first page and 2 computers from the third page, all 4 computers are removed.

## Comment

We found that 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 very convenient.

## Windows client protection software



Your computer is protected

Updating virus and spyware protection...

See how you are currently protected.

See what you can do with the program.

See what the program has done.

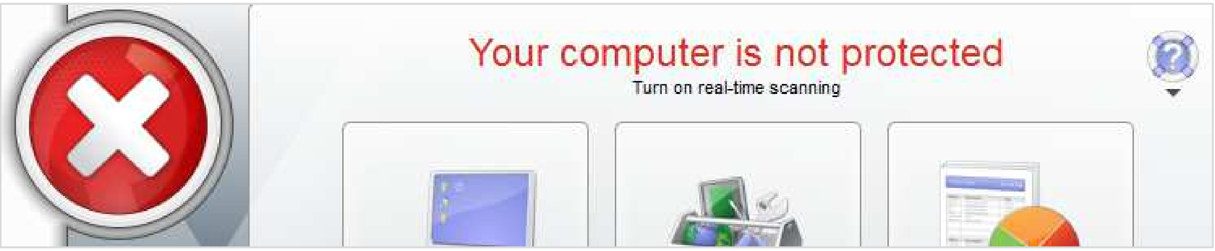
Protecting the irreplaceable

### Installation

A 100 MB .EXE installer file is downloaded from the console and run. The admin has to accept a licence agreement and enter an activation key. No further interaction is required.

### Main program window

This lets the user run updates and start scans. There is a status display in the form of a green icon and text when all is well; these turn red and show a warning if a protection component is disabled:



Your computer is not protected

Turn on real-time scanning

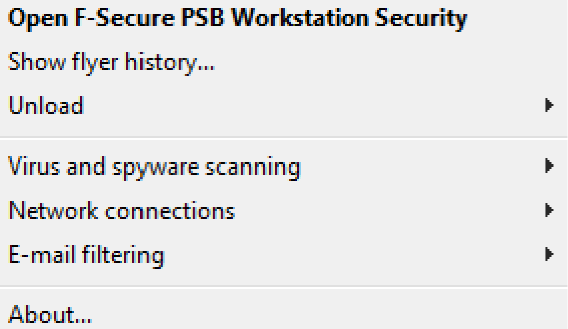
There is however no means of reactivating the protection easily, an admin or user who sees such an alert has to go into the settings to enable the relevant component.

### Windows Security Center/Windows Defender

F-Secure PSB Workstation Security registers as firewall, antivirus and antispyware in Windows Security Center. Under Windows 7, Windows Defender is not disabled.

## System Tray icon

A system tray icon is displayed, right-clicking which shows the following menu:

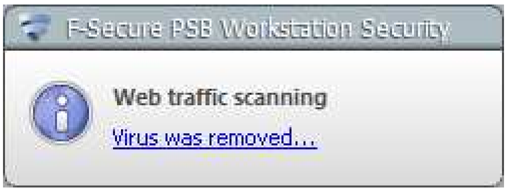


## Unauthorised access

We were able to deactivate the real-time protection in the settings using a standard user account.

## Malware alerts

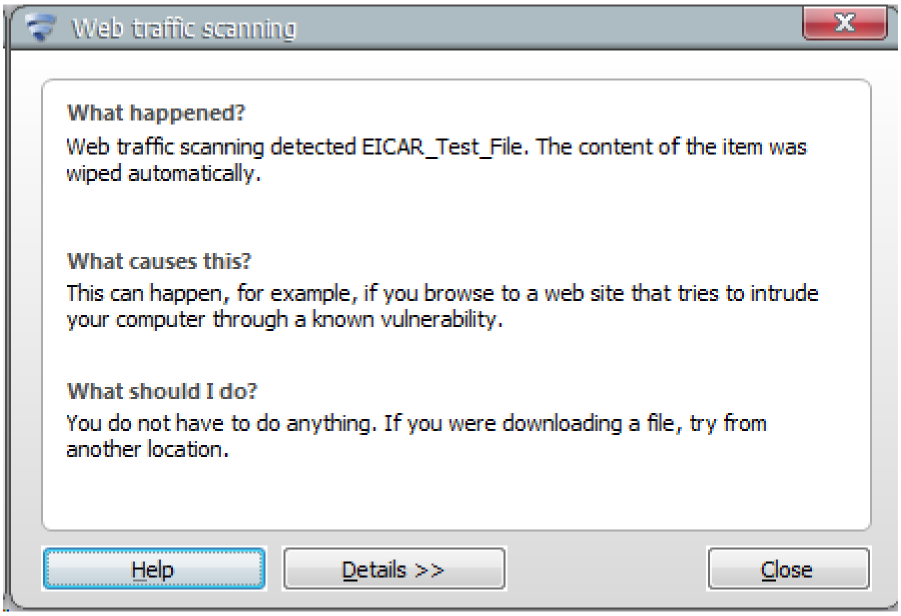
The following alert is shown if the EICAR test file is downloaded:



**Web traffic scanning**

Virus was removed...

Clicking *Virus was removed…* displays the following information:



**What happened?**

Web traffic scanning detected EICAR_Test_File. The content of the item was wiped automatically.

**What causes this?**

This can happen, for example, if you browse to a web site that tries to intrude your computer through a known vulnerability.

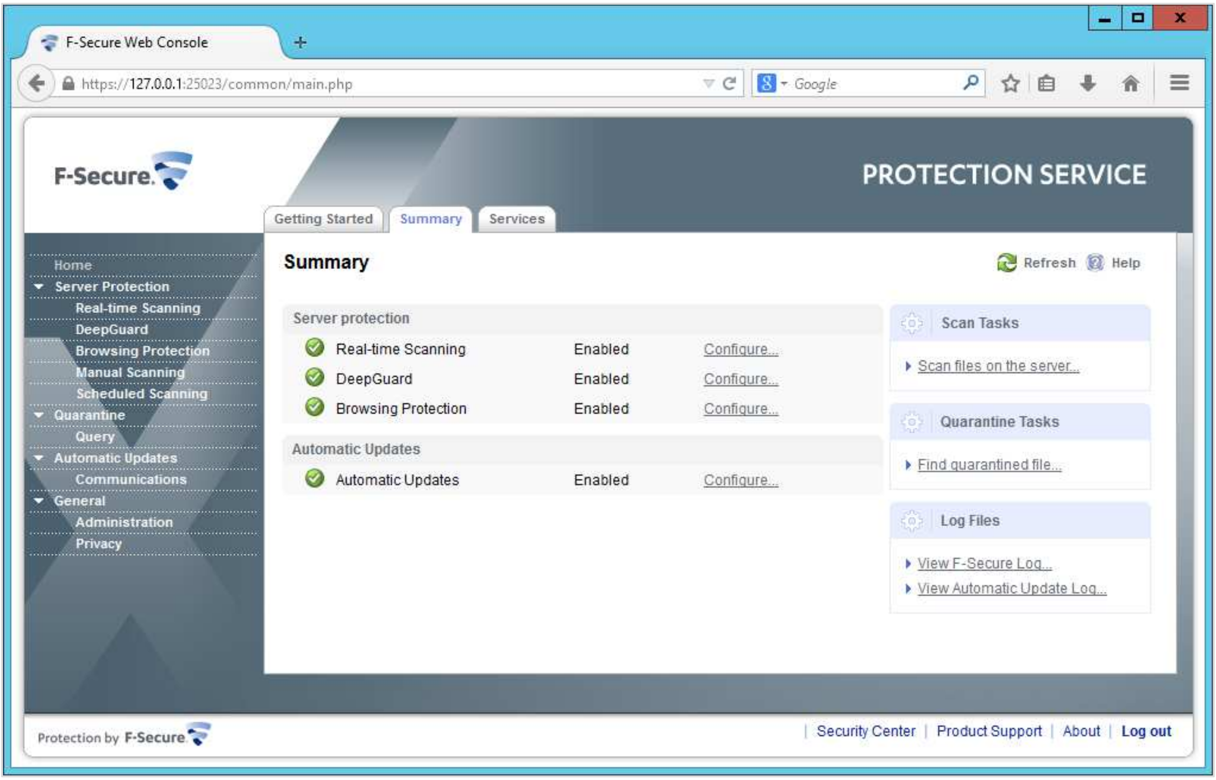
**What should I do?**

You do not have to do anything. If you were downloading a file, try from another location.

## Comment

The client software has a simple and familiar design, and allows users to run scans and updates, which we find sensible. We liked the user-friendly explanation when malware is detected. We recommend administrators to change the default policy that allows standard users to deactivate protection components. We also suggest providing a fix-all button to reactivate protection in the event that it has been disabled.

## Windows server protection software



Summary

Server protection

| | | |
|---|---|---|
| Real-time Scanning | Enabled | Configure... |
| DeepGuard | Enabled | Configure... |
| Browsing Protection | Enabled | Configure... |

Automatic Updates

| | | |
|---|---|---|
| Automatic Updates | Enabled | Configure... |

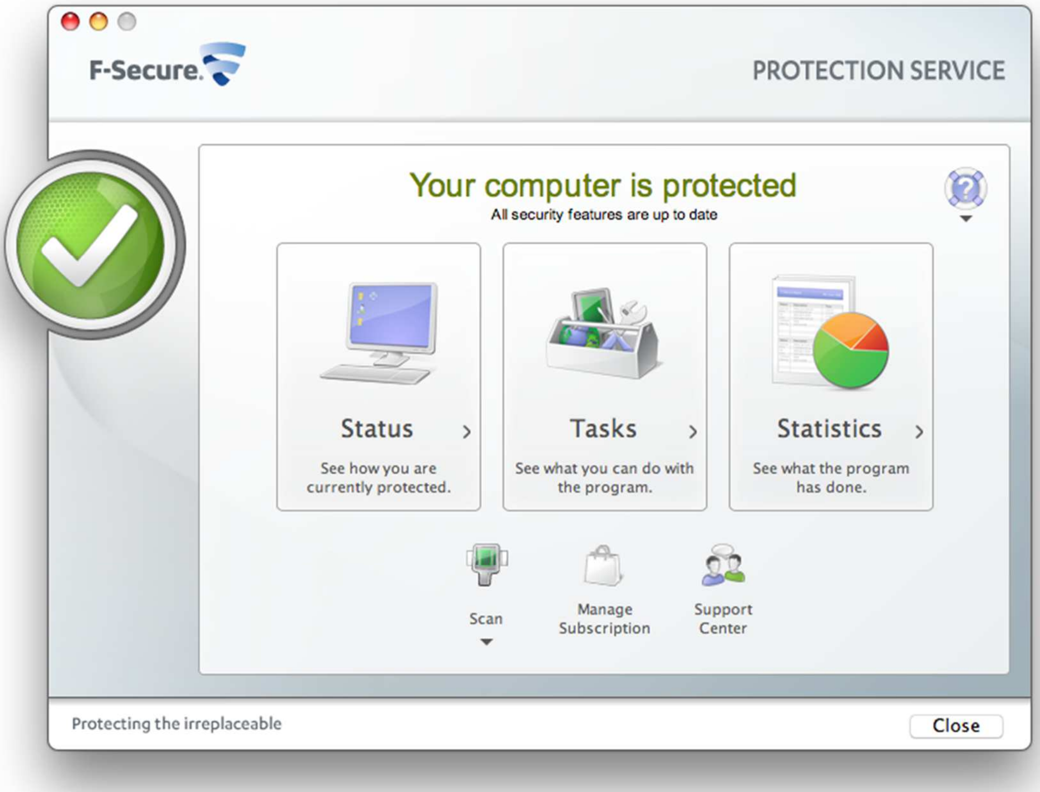
The file-server protection software has its own installation package, which can be downloaded from the console in just the same way as the client software. The setup wizard involves choosing the language, accepting a licence agreement, entering a subscription key, and choosing the location of the installation folder.

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 above, the interface has a status display and links to scans, quarantine, updates and settings.

### Comment

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, we feel that even non-expert admins should be able to manage the product without any difficulty.

## Mac client protection software


F-Secure
PROTECTION SERVICE
Your computer is protected
All security features are up to date
Status
See how you are currently protected.
Tasks
See what you can do with the program.
Statistics
See what the program has done.
Scan
Manage Subscription
Support Center
Protecting the irreplaceable
Close

### Installation

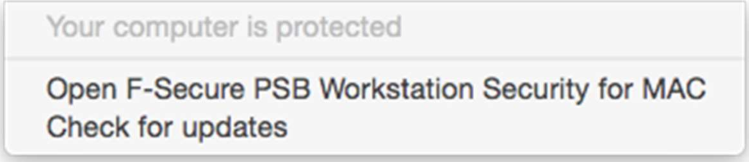
This involves running a .DMG installer file downloaded from the console, and accepting a licence agreement. No further interaction is required.

### Main program window

The main program window includes a scan menu and status display.

### System Tray icon

A System Tray icon is shown, which lets the user check status, open the program, or run an update:

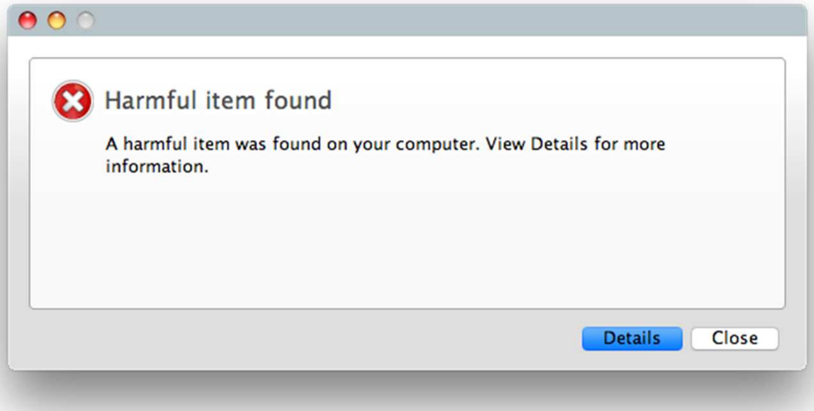

Your computer is protected
Open F-Secure PSB Workstation Security for MAC
Check for updates

### Unauthorised access

We could not find any means of disabling the protection from the client, even with an administrator account.

## Malware alerts

If the EICAR test file is downloaded, the following alert is displayed:



Harmful item found

A harmful item was found on your computer. View Details for more information.

Clicking *Details* shows the location of the detected item, and indicates that it has been trashed. The alert is displayed until the user closes it.

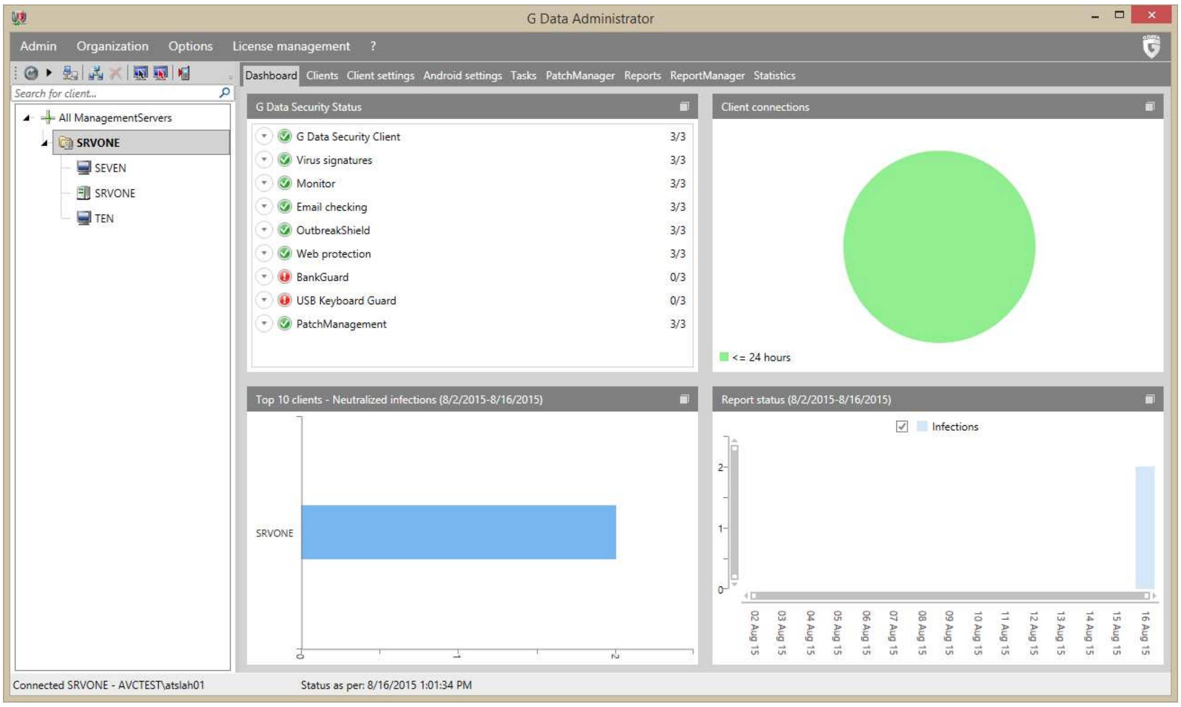
## Comment

We found the Mac protection software to have a simple and familiar design, which shows the status and allows users to run updates and scans.

## Summary

F-Secure Protection Service for Business is 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. Whilst we could suggest some minor modifications to the client software, overall we feel the product has been well designed, and makes monitoring and managing a small-business network very straightforward.

# G Data Antivirus Business



G Data Security Status

| | |
|---|---|
| ✓ G Data Security Client | 3/3 |
| ✓ Virus signatures | 3/3 |
| ✓ Monitor | 3/3 |
| ✓ Email checking | 3/3 |
| ✓ OutbreakShield | 3/3 |
| ✓ Web protection | 3/3 |
| ! BankGuard | 0/3 |
| ! USB Keyboard Guard | 0/3 |
| ✓ PatchManagement | 3/3 |

Connected SRVONE - AVCTEST\atslah01

Status as per: 8/16/2015 1:01:34 PM

## Introduction

G Data Antivirus Business uses an on-premise, Windows-based console to manage client devices (it can optionally be hosted on e.g. Microsoft Azure). G Data's business range also includes Client Security Business, which offers additional features such as a client firewall, and Endpoint Protection Business, which can additionally be provided as a service managed by a G Data Partner. The G Data Business products can be extended by adding optional modules such as MailSecurity, Client Backup and Patch Management.

## Software versions reviewed

G Data Administrator 13.2.0.2
Windows Security Client 13.2.0.257

## Supported operating systems

Windows clients: Windows XP (32-bit only), Vista, 7, 8, 8.1, 10
Windows servers: Windows Server 2003, 2008/R2, 2012/R2
Linux[11]
Android/iOS: please see feature list

## Documentation

### Manuals

The zip file containing the installation files very conveniently also includes a 149-page manual in .PDF format. This covers all aspects of installing and using the management console, including client deployment, configuration, monitoring and management. A 153-page Reference Guide is also available, which amongst other things provides an overview of G Data's business range, and advice to customers on choosing the right product for them.

[11] https://www.gdatasoftware.com/solutions-products/business/system-requirements

### Knowledge base

We could not find a knowledge base on the manufacturer's website. There is however an FAQ section in the manual.

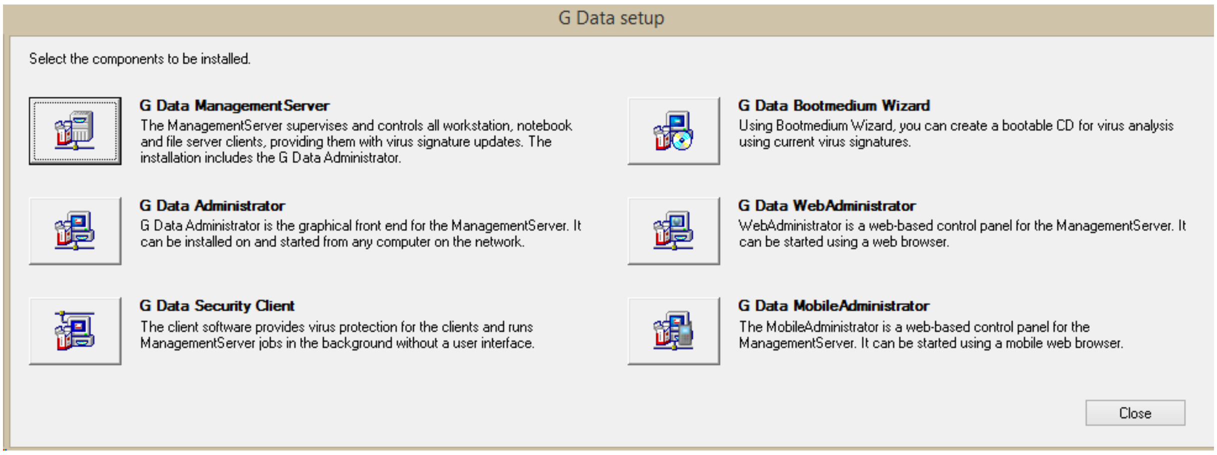
### Comment

The manual has been produced to a very high standard. We found it to be very clear and comprehensive, well laid-out, easily accessible via bookmarks and a clickable contents page, and well illustrated with screenshots.

## Management Console

### Installation and configuration

The console is installed on the management server by running the installer file, and choosing the *G Data Management Server* option:



G Data setup

Select the components to be installed.

**G Data ManagementServer**
The ManagementServer supervises and controls all workstation, notebook and file server clients, providing them with virus signature updates. The installation includes the G Data Administrator.

**G Data Bootmedium Wizard**
Using Bootmedium Wizard, you can create a bootable CD for virus analysis using current virus signatures.

**G Data Administrator**
G Data Administrator is the graphical front end for the ManagementServer. It can be installed on and started from any computer on the network.

**G Data WebAdministrator**
WebAdministrator is a web-based control panel for the ManagementServer. It can be started using a web browser.

**G Data Security Client**
The client software provides virus protection for the clients and runs ManagementServer jobs in the background without a user interface.

**G Data MobileAdministrator**
The MobileAdministrator is a web-based control panel for the ManagementServer. It can be started using a mobile web browser.

The console setup wizard then runs. This involves accepting a licence agreement, choosing the location of the installation folder, selecting main/secondary/subnet server, and whether to use Microsoft SQL Express (included) or an existing SQL installation. SQL Express is recommended for networks with up to 1,000 clients, and so we used this. The G Data software has to be activated using a licence key or access data at the end of the setup process, and then the server needs to be restarted. We found the procedure to be quick and straightforward.

We note that the G Data Management Server runs as a Windows Service of the same name. By default, this is set to Automatic (Delayed Start); after the PC running the Management Server is started/restarted, the administrator may have to wait a minute or two before being able to log in.

### Layout

The G Data Administrator console has a similar layout to the Microsoft Management Console, with a narrow left-hand pane displaying the names of the server(s) and clients, and a larger right-hand pane showing various details of the selected device or group.

### Preparing devices for deployment

In accordance with the instructions in the product manual, we opened firewall ports 7161, 7182, 7183 and 7184 on the server, and port 7169 on the Windows clients. Additional steps needed for remote installation are also described in the manual.

## Deploying the endpoint protection software

The client software can be deployed by remote push installation, or local installation, which can be performed using logon script, group policy, or manually. We used the last of these in our test.

## Monitoring the network

### *Status*

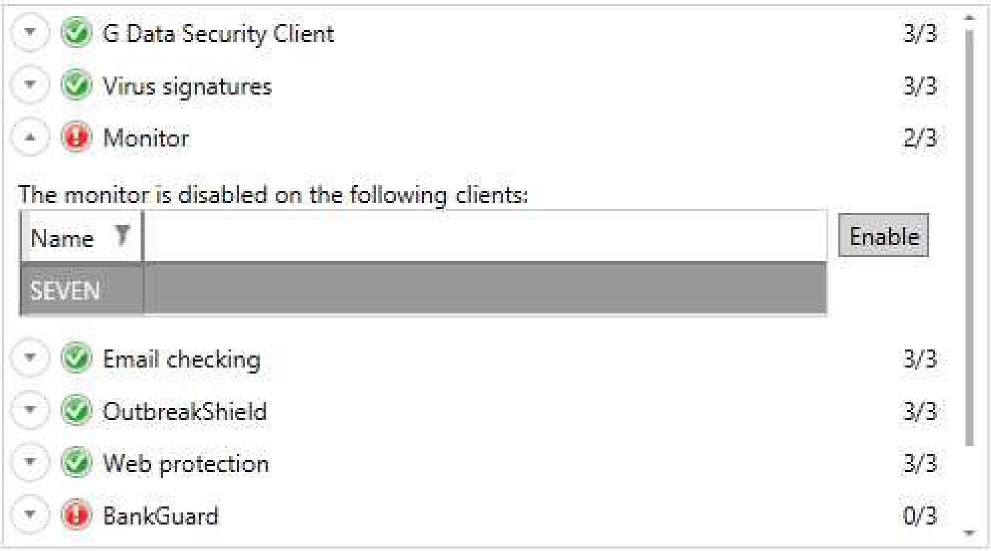
The status of devices on the network is shown in the *G Data Security Status* panel on the dashboard. This provides a very detailed overview by listing the individual protection components, and showing how many of the total number of devices conform to optimal settings.

### *Warnings*

Components which are not installed, or not configured correctly, are shown with an exclamation mark symbol in a red circle.

### *Rectifying problems*

Clicking on an item shown to be non-functional or incorrectly configured shows the individual devices affected, and allows the administrator to solve the problem by selecting the device(s) concerned and clicking *Enable*:



| | |
|---|---|
| ✓ G Data Security Client | 3/3 |
| ✓ Virus signatures | 3/3 |
| ! Monitor | 2/3 |

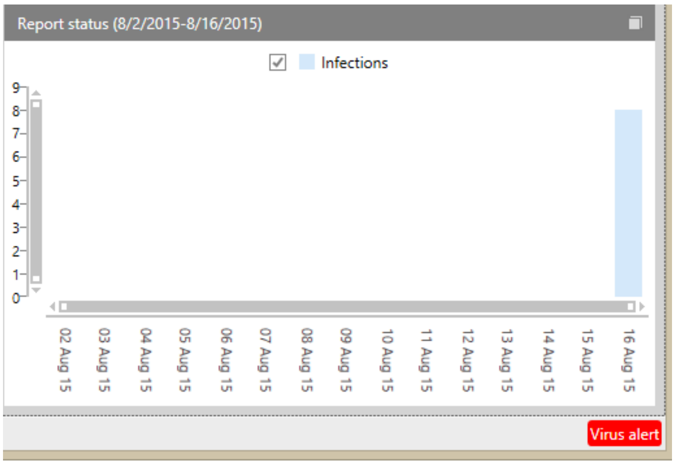
The monitor is disabled on the following clients:

| Name |
|---|
| SEVEN |

| | |
|---|---|
| ✓ Email checking | 3/3 |
| ✓ OutbreakShield | 3/3 |
| ✓ Web protection | 3/3 |
| ! BankGuard | 0/3 |

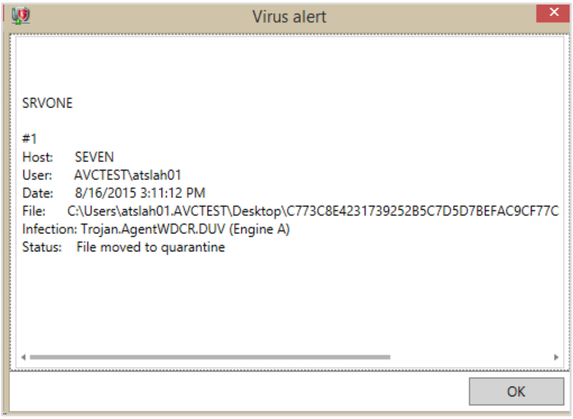
### *Malware alerts*

When malware is detected on a client, an alert is shown in the bottom right-hand corner of the console window:



Report status (8/2/2015-8/16/2015)

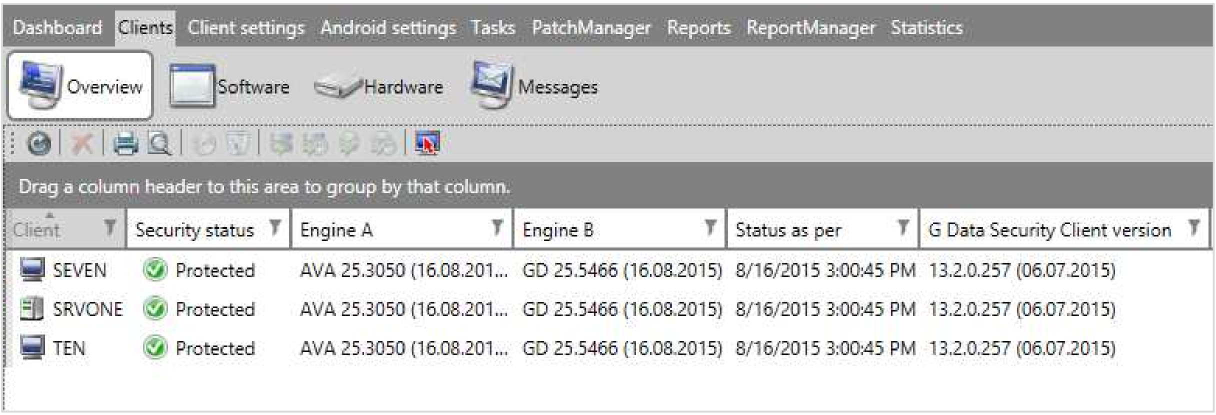
Double-clicking this displays a message box with the details:



```
SRVONE

#1
Host:     SEVEN
User:     AVCTEST\atslah01
Date:     8/16/2015 3:11:12 PM
File:    C:\Users\atslah01.AVCTEST\Desktop\C773C8E4231739252B5C7D5D7BEFAC9CF77C
Infection: Trojan.AgentWDCR.DUV (Engine A)
Status:   File moved to quarantine
```

*Program version*

This can be seen by clicking *Overview/Clients:*



| Client | Security status | Engine A | Engine B | Status as per | G Data Security Client version |
|---|---|---|---|---|---|
| SEVEN | ✓ Protected | AVA 25.3050 (16.08.201... | GD 25.5466 (16.08.2015) | 8/16/2015 3:00:45 PM | 13.2.0.257 (06.07.2015) |
| SRVONE | ✓ Protected | AVA 25.3050 (16.08.201... | GD 25.5466 (16.08.2015) | 8/16/2015 3:00:45 PM | 13.2.0.257 (06.07.2015) |
| TEN | ✓ Protected | AVA 25.3050 (16.08.201... | GD 25.5466 (16.08.2015) | 8/16/2015 3:00:45 PM | 13.2.0.257 (06.07.2015) |

## Managing the network

### *Scanning*

Individual scans are run by selecting the client or group from the left-hand panel, then clicking the *Tasks* tab and the *Single Scan Job* icon on the toolbar below.

### *Scheduling Scans*

The procedure is identical for an individual scan, except that the admin clicks the *Periodic Scan Job* icon on the toolbar.

### *Updates*

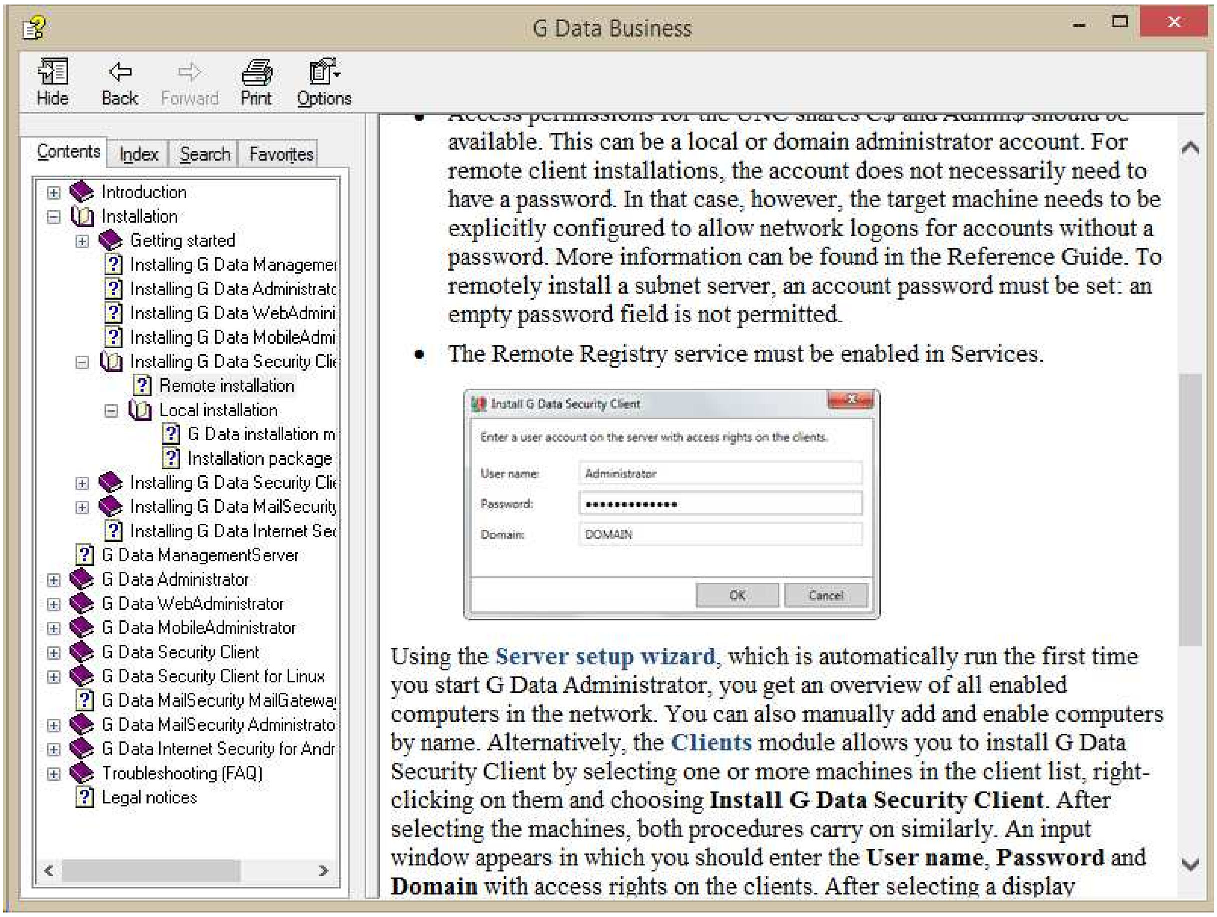
Updates can be run by clicking the *Clients* tab, selecting the device(s) to be updated, right-clicking and selecting *Update Virus Signatures Now*.

### *Removing devices from the console*

A device can be removed by right-clicking it (e.g. in the *Clients* view shown above) and then clicking *Delete*.

## Integrated help feature

A comprehensive Windows Help file is provided, covering all aspects of using the console. Instructions are illustrated with some screenshots:


G Data Business
Hide
Back
Forward
Print
Options
Contents
Index
Search
Favorites
Introduction
Installation
Getting started
Installing G Data Managemer
Installing G Data Administratc
Installing G Data WebAdmini
Installing G Data MobileAdmi
Installing G Data Security Clie
Remote installation
Local installation
G Data installation m
Installation package
Installing G Data Security Clie
Installing G Data MailSecurity
Installing G Data Internet Sec
G Data ManagementServer
G Data Administrator
G Data WebAdministrator
G Data MobileAdministrator
G Data Security Client
G Data Security Client for Linux
G Data MailSecurity MailGatewa
G Data MailSecurity Administrato
G Data Internet Security for Andr
Troubleshooting (FAQ)
Legal notices

- Access permissions for the UNC shares C$ and Admin$ should be available. This can be a local or domain administrator account. For remote client installations, the account does not necessarily need to have a password. In that case, however, the target machine needs to be explicitly configured to allow network logons for accounts without a password. More information can be found in the Reference Guide. To remotely install a subnet server, an account password must be set: an empty password field is not permitted.
- The Remote Registry service must be enabled in Services.

Install G Data Security Client

Enter a user account on the server with access rights on the clients.

User name: Administrator
Password: ••••••••••••••
Domain: DOMAIN

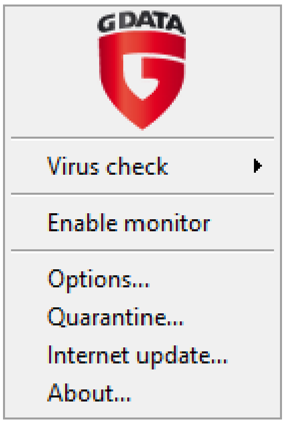
OK Cancel

Using the **Server setup wizard**, which is automatically run the first time you start G Data Administrator, you get an overview of all enabled computers in the network. You can also manually add and enable computers by name. Alternatively, the **Clients** module allows you to install G Data Security Client by selecting one or more machines in the client list, right-clicking on them and choosing **Install G Data Security Client**. After selecting the machines, both procedures carry on similarly. An input window appears in which you should enter the **User name**, **Password** and **Domain** with access rights on the clients. After selecting a display

## Comment

We found the G Data Administrator management console to be very intuitive to use, especially for someone who is familiar with Microsoft administration tools such as the Microsoft Management console. We were able to find essential information and functionality very quickly and easily. The status display struck us as very informative, with its listing of individual components, and makes rectifying problems very easy.

## Windows client protection software

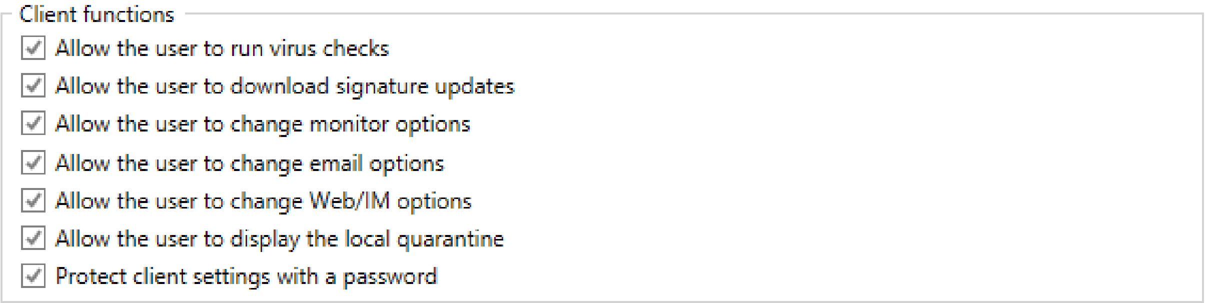


### Installation

The software can be installed by running the same installer file used for the console, but in this case selecting G Data Security Client. The setup wizard is very simple, the admin only needs to accept a licence agreement and enter the name of the management server. The client software is then automatically registered with the console.

### Main program window

The G Data Security Client does not have a program window as such. The interface consists of the System Tray icon's menu, shown above. By default, this only displays the entries *Internet Update* and *About*. The functionality available to the user can be extended from the console, so that the user can run scans, change options and display the quarantine:



Client functions

☑ Allow the user to run virus checks
☑ Allow the user to download signature updates
☑ Allow the user to change monitor options
☑ Allow the user to change email options
☑ Allow the user to change Web/IM options
☑ Allow the user to display the local quarantine
☑ Protect client settings with a password

We note that the administrator can password protect the settings if desired.

### Windows Security Center/Windows Defender

The client security software registers in Windows Security Center as antivirus and antispyware. Under Windows 7, Windows Defender is not disabled.

### System Tray icon

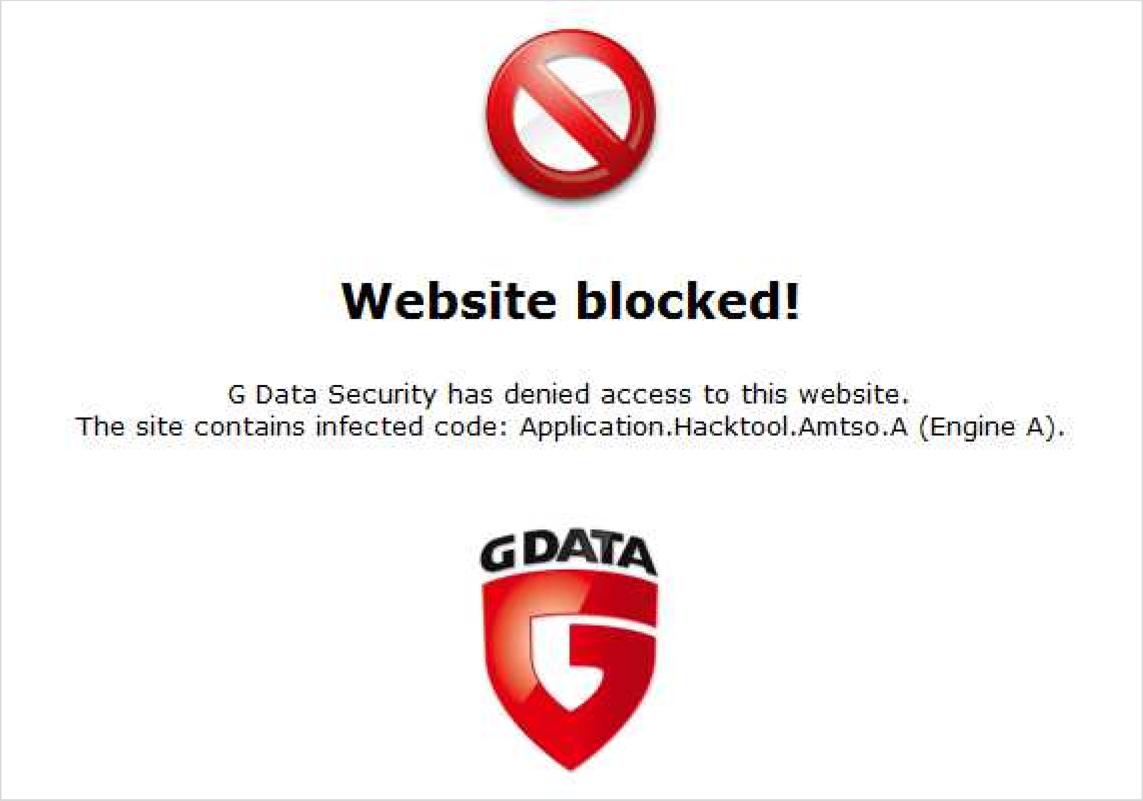
This is displayed, and provides the only means of local access to the client software.

### Unauthorised access

This is effectively prevented. The default interface does not allow the user – regardless of privileges – to alter the configuration at all. Using the options shown above, the administrator can allow user to change settings, but limit this to certain individuals by means of setting a password.

### Malware alerts

The following alert is shown in the browser window when malware is discovered:



Website blocked!

G Data Security has denied access to this website.
The site contains infected code: Application.Hacktool.Amtso.A (Engine A).

### Windows server protection software

In terms of interface and available functionality, this can be regarded as being identical to the client software.

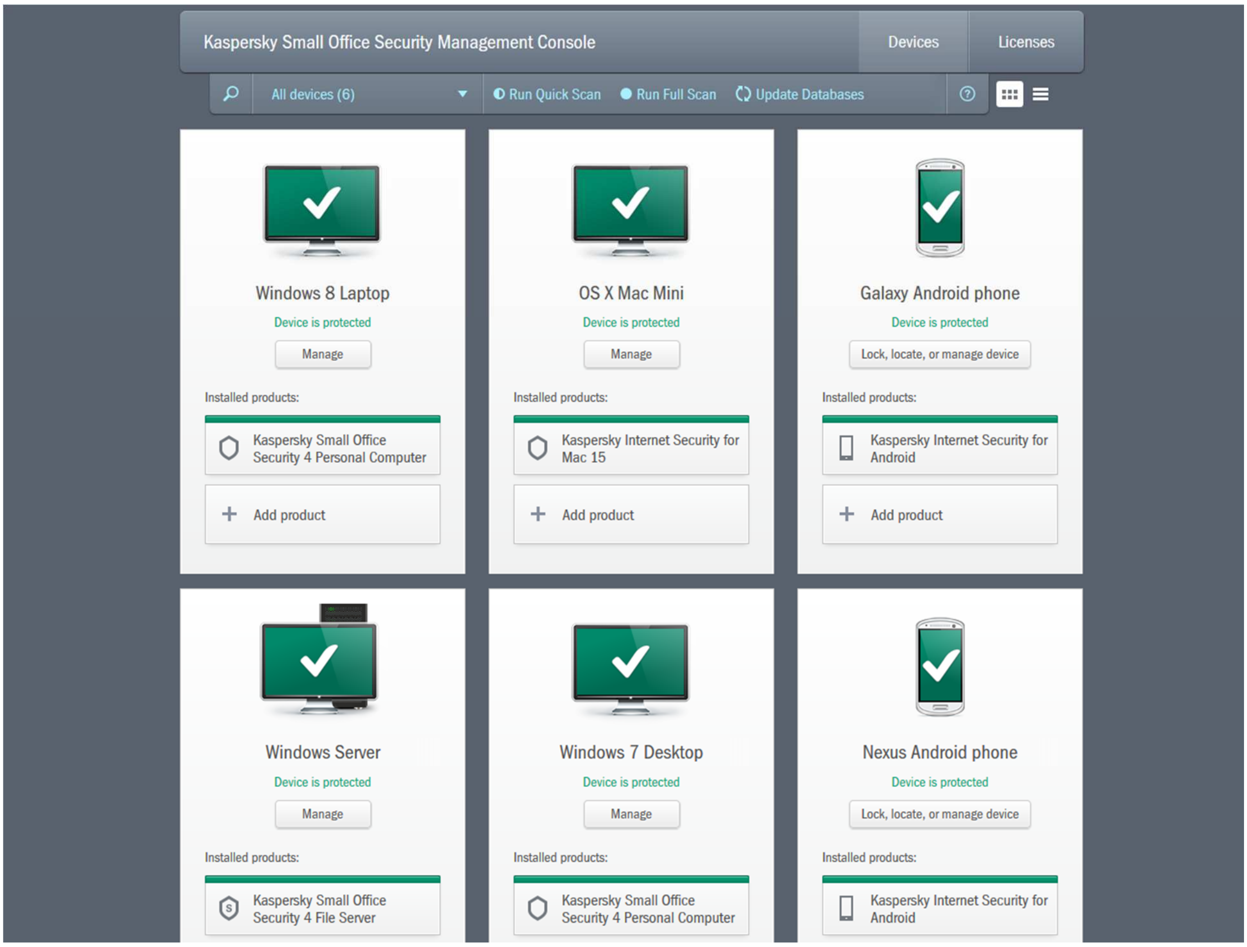
### Comment

Although the minimalist user interface of the software will appear unusual to some people, it prevents unauthorised access, and the administrator can let users perform basic tasks if so desired. In practical terms, we would say that it has been well designed.

### Summary

For experienced IT professionals, G Data Antivirus Business is very intuitive and straightforward to install and manage. SQL Express installation is seamlessly integrated into the console setup wizard, and the console will be very familiar to anyone who is used to e.g. the Microsoft Management Console. The minimalist interface of the client software may be unusual, but works very well from a practical point of view. Whilst small businesses may find it easier to have an IT consultant perform the initial setup, we feel the console is so clear and intuitive to use that only minimal training would be necessary for a non-expert administrator to carry out everyday monitoring and management tasks. The excellent manual can be relied upon for further assistance.

## Kaspersky Small Office Security 4



### Introduction

Kaspersky Small Office Security 4 is a security package designed for small businesses with up to 25 desktop/laptops computers, especially those without professional IT support. It provides protection for Windows Servers, Windows desktops and laptops, Mac OS X desktops and laptops and Android Phones/Tablets, all managed via a cloud-based console.

For larger businesses and businesses with advanced demands, Kaspersky make two additional products: Endpoint Security for Business (in Core, Select and Advanced variants), and Total Security for Business.

### Software versions reviewed

Kaspersky Small Office Security Management Console as at June 2015
Kaspersky Small Office Security 4 File Server 15.0.2
Kaspersky Small Office Security 4 Personal Computer 15.0.2
Kaspersky Internet Security for Mac 15.0.1

## Supported operating systems

Windows clients: Windows XP, Vista, 7, 8, 8.1, 10[12], all in 32 and 64-bit versions
Windows servers: Windows Server 2008 R2, 2012, 2012 R2; Windows Small Business Server 2008, 2011
Mac OS X clients: OS X 10.7, 10.8, 10.9, 10.10
Android/iOS: please see feature list

## Documentation

We could not find a manual or any articles in the knowledge base relating to the Small Office Security console. However, assistance is provided in the form of the built-in help feature described below.

### Comment

Although the Kaspersky Small Office Security console is very easy to navigate and use, we nonetheless feel that a manual and/or knowledge base articles would be helpful.

[12] At the time of writing (late August 2015), the Kaspersky Lab website notes that some additional features of the Windows client, such as webcam protection, may not be fully operational under Windows 10

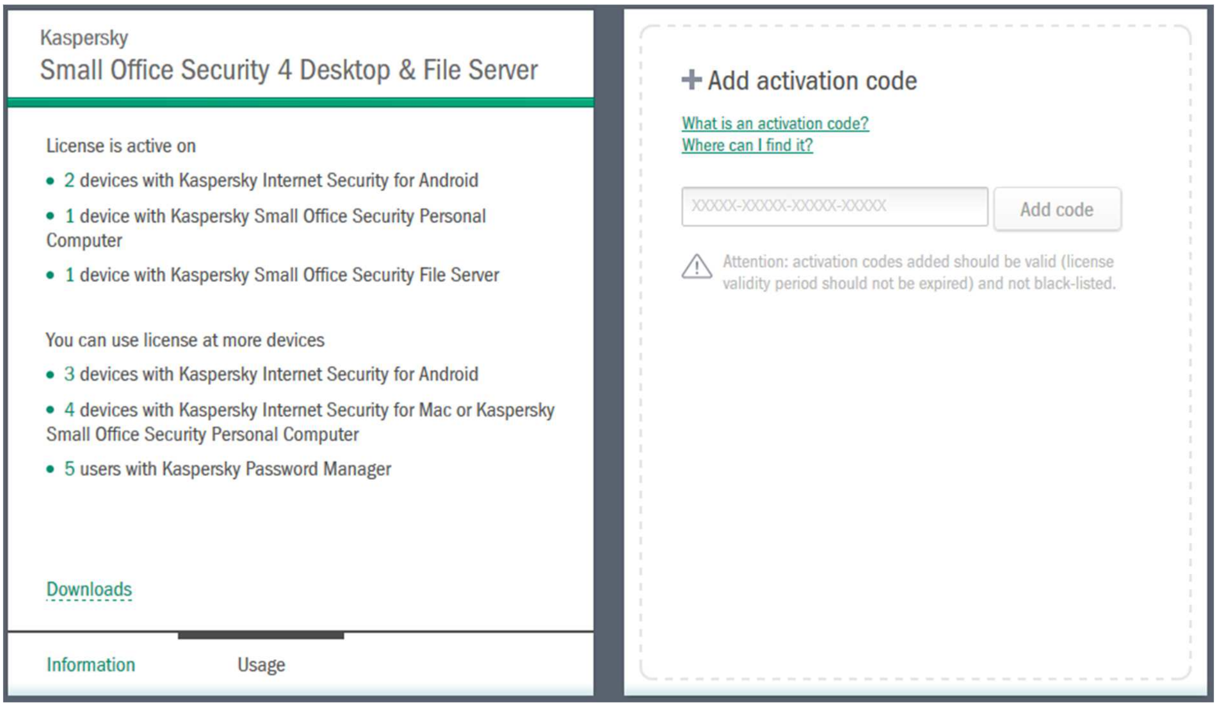
## Management Console

### Installation and configuration

The console is cloud-based, meaning that there is no installation required.

### Layout

The console has two main pages, *Devices* (shown by default) and *Licenses*. The administrator can switch between the pages using the two big buttons at the top. The *Usage* view of the *Licences* page shows the number of licences being used, and how many are still available; there is also a convenient link to the *Downloads* page, from which client protection software can be installed:



Kaspersky
Small Office Security 4 Desktop & File Server

License is active on

- 2 devices with Kaspersky Internet Security for Android
- 1 device with Kaspersky Small Office Security Personal Computer
- 1 device with Kaspersky Small Office Security File Server

You can use license at more devices

- 3 devices with Kaspersky Internet Security for Android
- 4 devices with Kaspersky Internet Security for Mac or Kaspersky Small Office Security Personal Computer
- 5 users with Kaspersky Password Manager

Downloads

Information Usage

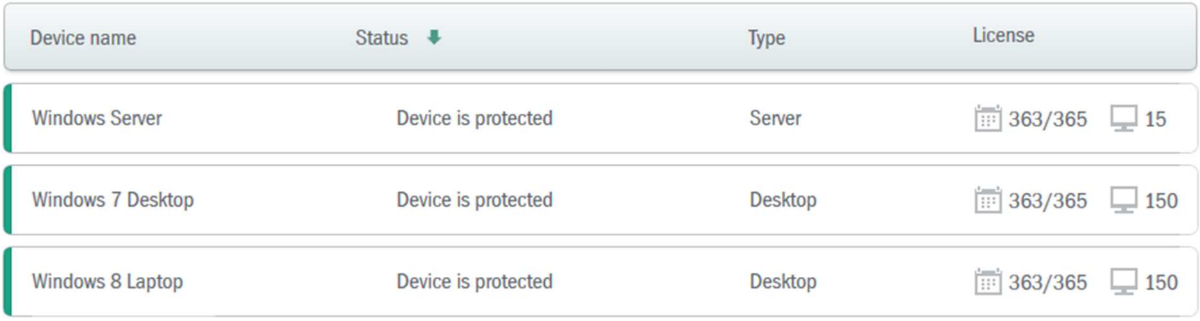
+ Add activation code

What is an activation code?
Where can I find it?

XXXXX-XXXXX-XXXXX-XXXXX Add code

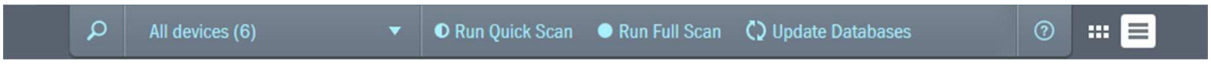
Attention: activation codes added should be valid (license validity period should not be expired) and not black-listed.

The *Devices* page displays all the protected devices. These can be shown as tiles, with detailed information (as shown in the main screenshot at the start of this report), or in the form of a list, as shown below:



| Device name | Status | Type | License |
|---|---|---|---|
| Windows Server | Device is protected | Server | 363/365 15 |
| Windows 7 Desktop | Device is protected | Desktop | 363/365 150 |
| Windows 8 Laptop | Device is protected | Desktop | 363/365 150 |

A menu bar at the top of the page allows the administrator to toggle between these two views, filter the devices shown, carry out common tasks such as scans and updates, and open the help feature:

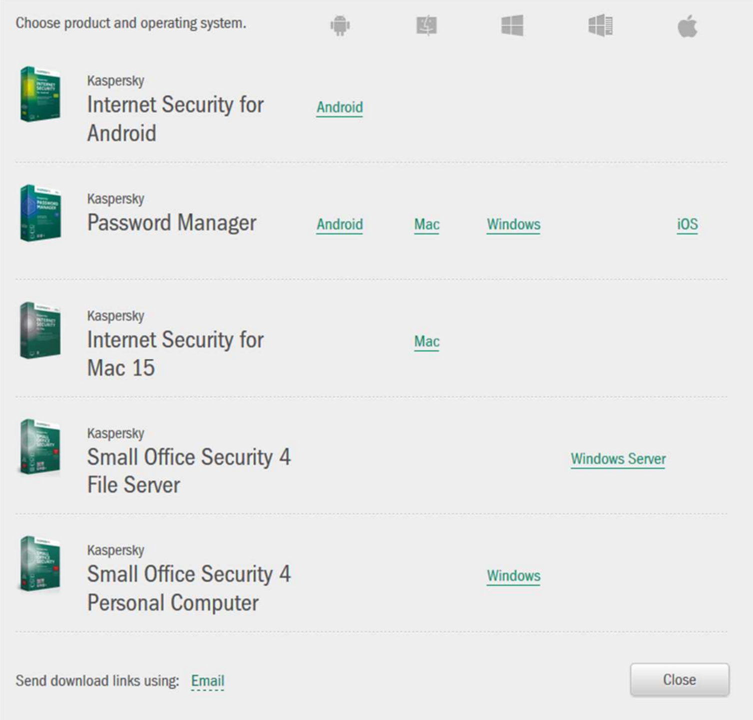


### Preparing devices for deployment

No specific preparations are needed on any compatible device, other than removing any existing security software.

## Deploying the endpoint protection software

To deploy protection software to devices, the administrator opens the *Downloads* page, which displays links for all the available products:



| Choose product and operating system. | | | | | |
|---|---|---|---|---|---|
| Kaspersky<br>Internet Security for Android | Android | | | | |
| Kaspersky<br>Password Manager | Android | Mac | Windows | | iOS |
| Kaspersky<br>Internet Security for Mac 15 | | Mac | | | |
| Kaspersky<br>Small Office Security 4 File Server | | | | Windows Server | |
| Kaspersky<br>Small Office Security 4 Personal Computer | | | Windows | | |

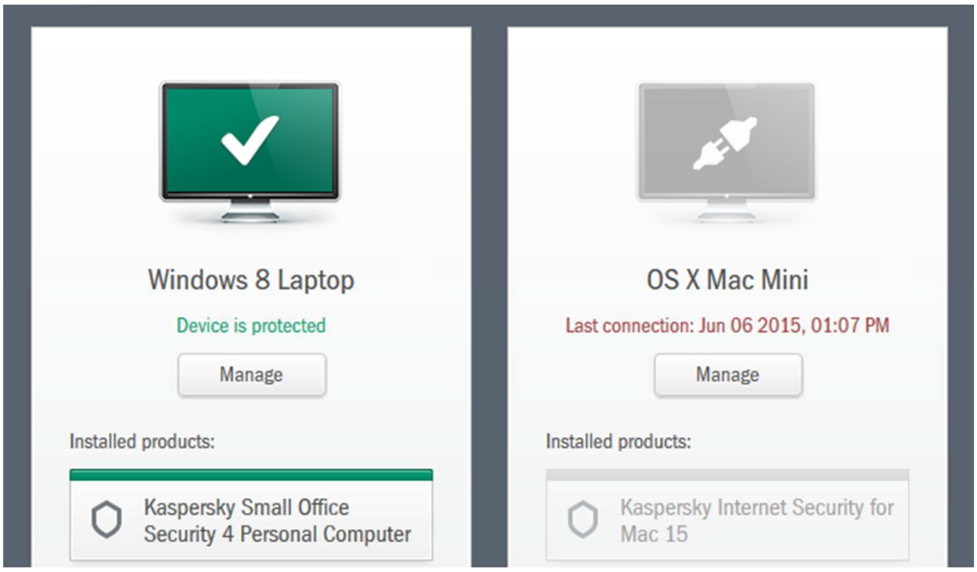
Send download links using: Email

The software can be deployed to all devices either by clicking the appropriate link, or by sending an email to remote users so that they can install the software themselves. For Windows and Mac OS X computers, the respective installer file can be downloaded once, and then copied to a flash drive or network share to install further machines.

## Monitoring the network

### *Status*

The *Devices* view of the console gives a simple, at-a-glance view of the status of the company's devices. For each device, there is an icon and caption which serve as the status display:



Windows 8 Laptop

Device is protected

Installed products:

Kaspersky Small Office Security 4 Personal Computer

OS X Mac Mini

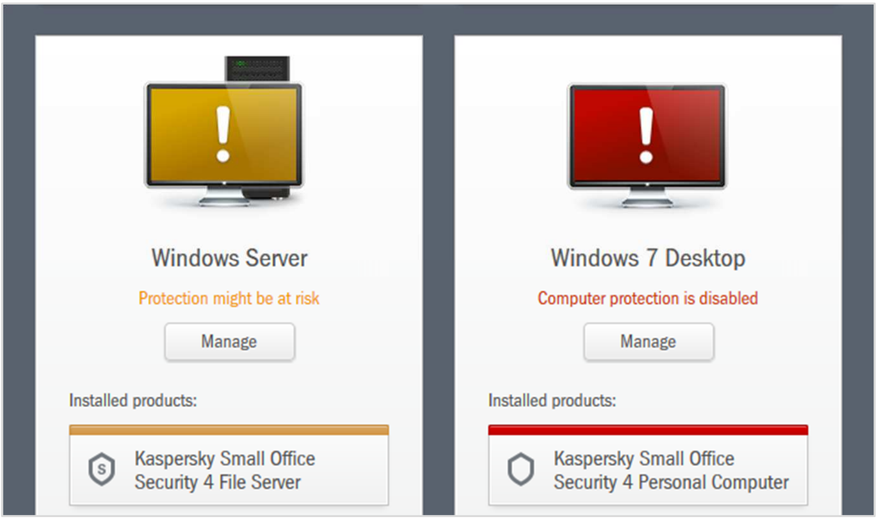
Last connection: Jun 06 2015, 01:07 PM

Installed products:

Kaspersky Internet Security for Mac 15

### *Warnings*

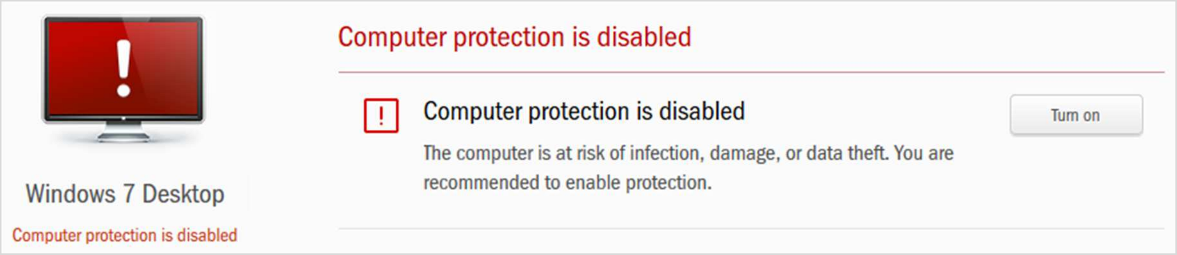
Warnings are shown very clearly by the icon and its caption:



Windows Server
Protection might be at risk
Manage
Installed products:
Kaspersky Small Office Security 4 File Server
Windows 7 Desktop
Computer protection is disabled
Manage
Installed products:
Kaspersky Small Office Security 4 Personal Computer

### *Rectifying problems*

To correct a problem shown for any device – Windows or Mac – the administrator clicks *Manage*; this opens the device's details page, which provides a more detailed explanation, a recommended course of action, and the means to carry this out. The details page for the PC with disabled protection is shown below. Simply clicking the *Turn on* button reactivates the protection.



Computer protection is disabled

Computer protection is disabled

The computer is at risk of infection, damage, or data theft. You are recommended to enable protection.

### *Malware alerts*

If Kaspersky Small Office Security endpoint protection software detects and completely eliminates a threat, as it does with the EICAR test file, no warning is shown in the console, as no action is required of the administrator.

### *Program version*

Whilst every device's tile shows the Kaspersky Lab product(s) installed, the administrator has to check the device locally to determine the exact program version.

## Managing the network

### *Scanning*

To run a scan on all the devices on the network, the administrator simply clicks *Run Quick Scan* or *Run Full Scan*, as appropriate, on the *Devices* page of the console.

### *Scheduling Scans*

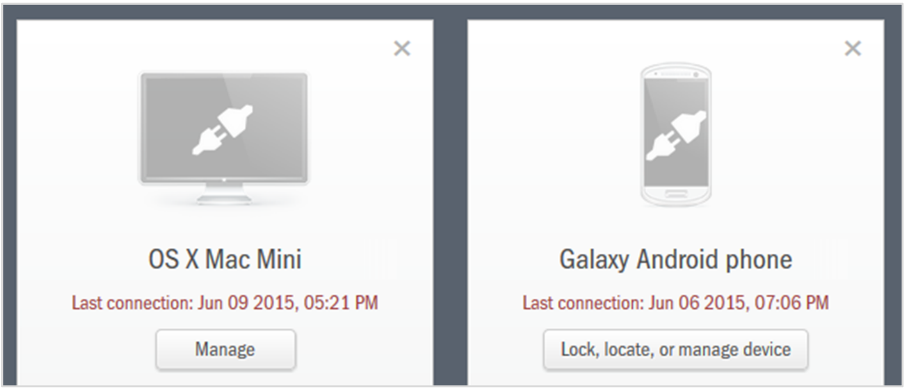
It is not possible to set a scanning schedule from the console, but this can be done on the individual PC/Server.

### *Updates*

The process for running updates is exactly parallel to running a scan, both for all devices or just one, using the relevant *Update* button.

### *Removing devices from the console*

If a device has been inactive (not communicated with the console) for 4 days, an *X* symbol appears in the top right-hand corner of its tile; clicking this allows the device to be hidden from the console. This has to be confirmed, to prevent it happening by accident.



OS X Mac Mini

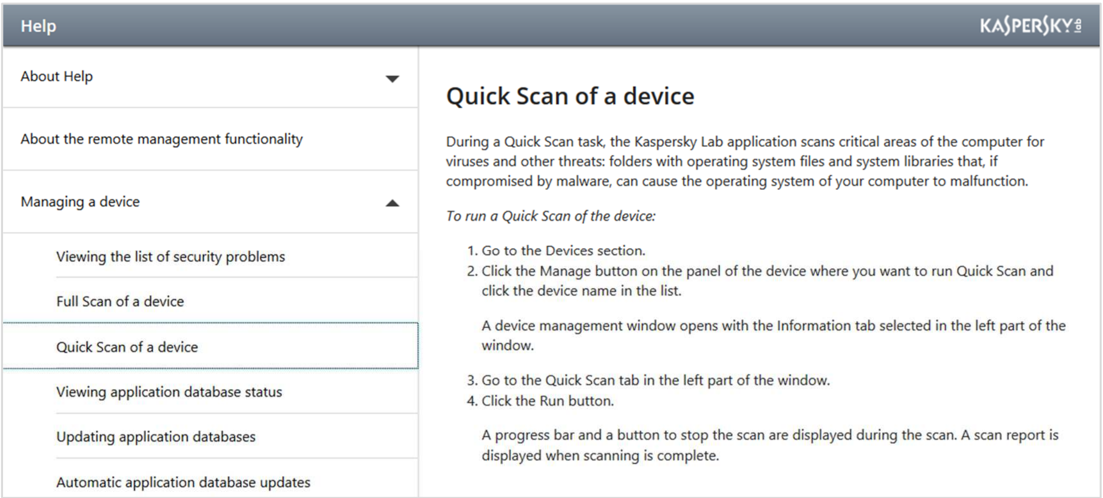
Last connection: Jun 09 2015, 05:21 PM

Galaxy Android phone

Last connection: Jun 06 2015, 07:06 PM

### Integrated help feature

Clicking the *?* symbol in the top right-hand corner of the console opens the help pages in a new tab of the browser. These provide a clear overview of main topics on the left, with instructions for each topic on the right. We note that the layout is very tablet-friendly, with the topics list easy to tap with a finger, and very concise instructions that can be displayed in a legible size on a small tablet screen without too much scrolling being required.



Help
KASPERSKY
About Help
About the remote management functionality
Managing a device
Viewing the list of security problems
Full Scan of a device
Quick Scan of a device
Viewing application database status
Updating application databases
Automatic application database updates

Quick Scan of a device

During a Quick Scan task, the Kaspersky Lab application scans critical areas of the computer for viruses and other threats: folders with operating system files and system libraries that, if compromised by malware, can cause the operating system of your computer to malfunction.

*To run a Quick Scan of the device:*

1. Go to the Devices section.
2. Click the Manage button on the panel of the device where you want to run Quick Scan and click the device name in the list.

   A device management window opens with the Information tab selected in the left part of the window.

3. Go to the Quick Scan tab in the left part of the window.
4. Click the Run button.

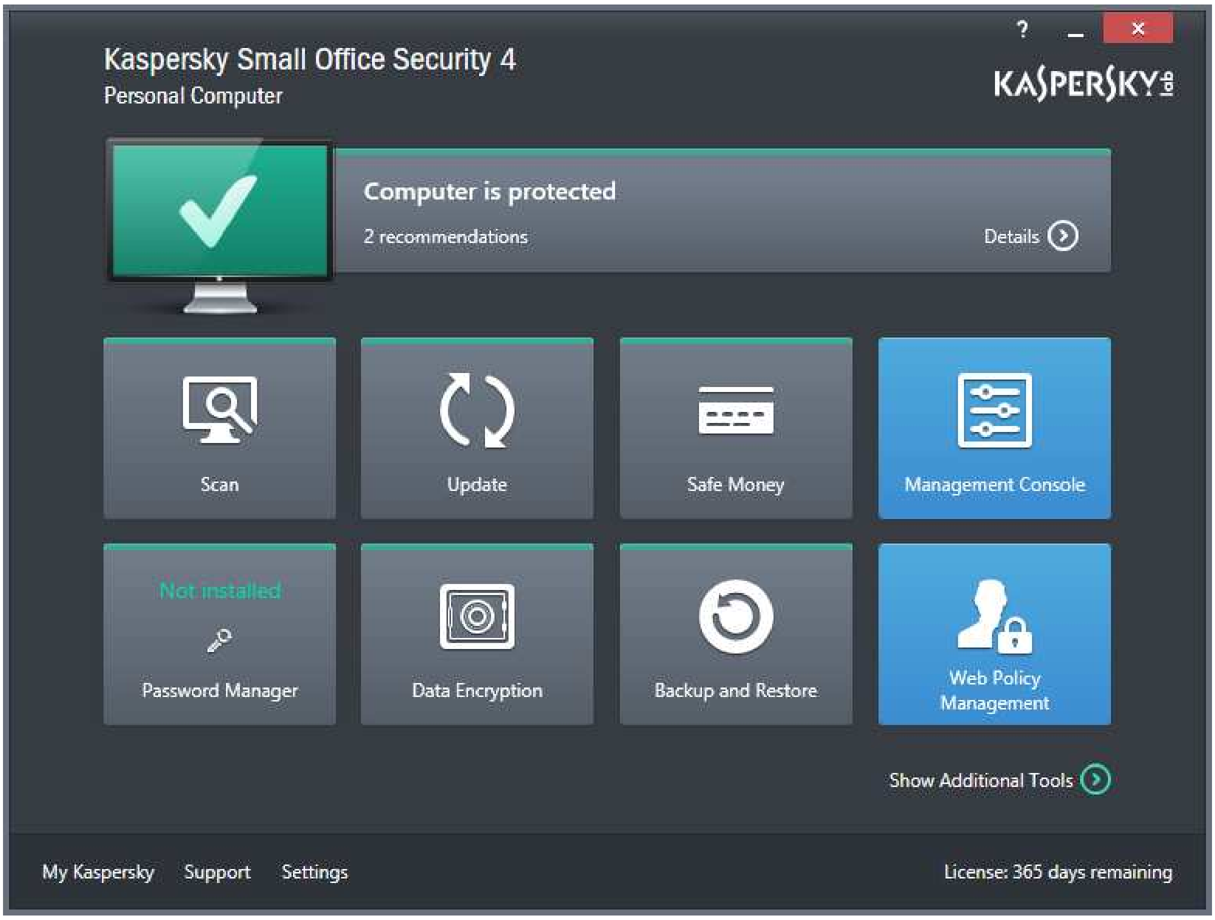
   A progress bar and a button to stop the scan are displayed during the scan. A scan report is displayed when scanning is complete.

### Comment

We were struck by the simplicity of the console design, which allows the status of all devices to be seen clearly, and essential tasks such as updates and scans to be carried out, from a single page. We feel that this would enable somebody new to network security management to find their way around easily without any training.

We have one suggestion for improvement. To get to the *Downloads* page to deploy software, the administrator has to click on *Licenses* and then *Usage*; we did not find this very intuitive, and suggest that a link could be added to the console in a more prominent position.

## Windows client protection software

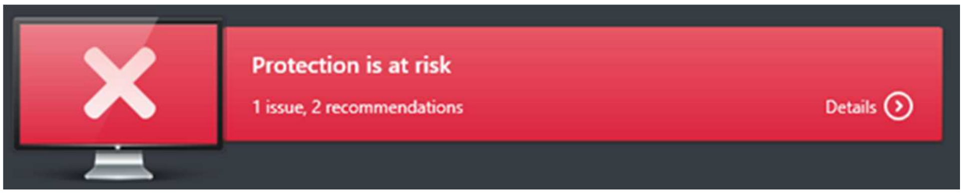


### Installation

Clicking the relevant link in the console/email downloads an exe setup file, which is then run on the target machine. The administrator clicks one button *Install*, then just has to decide whether to join the Kaspersky Security Network.

### Main program window

The features status, update and scan all feature their own prominent tiles, and help, support, settings and licence information are all easily accessible from the home page. If protection is disabled, the status display shows a very prominent warning:



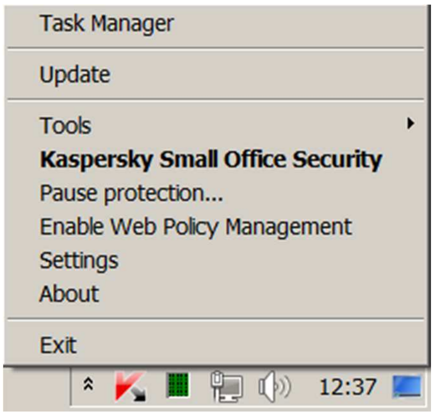
Clicking on the status display bar opens the Notification Center, from which the protection can be re-enabled.

### Windows Action Center

KSOS registers with Windows Action Center as the antivirus, antispyware and firewall.

### System Tray icon

An icon is displayed in the Windows System Tray. It can be double-clicked to open the main program window, or right-clicked to show a context menu of common tasks:

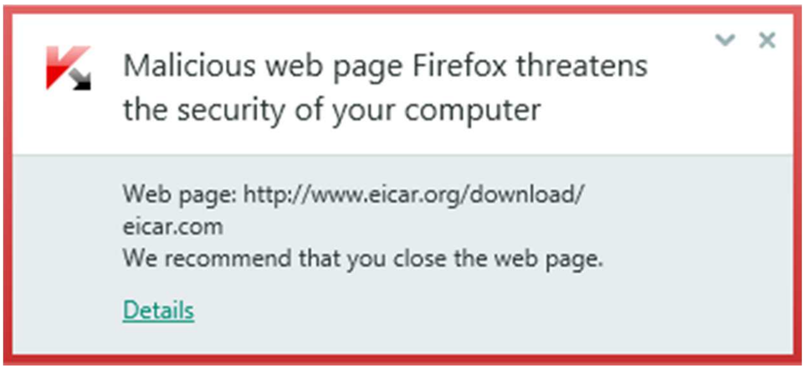


### Unauthorised access

The software can be password protected to prevent unauthorised access; we would strongly recommend administrators to activate this.

### Malware alerts

The following alert is shown if the user attempts to download the EICAR test file:

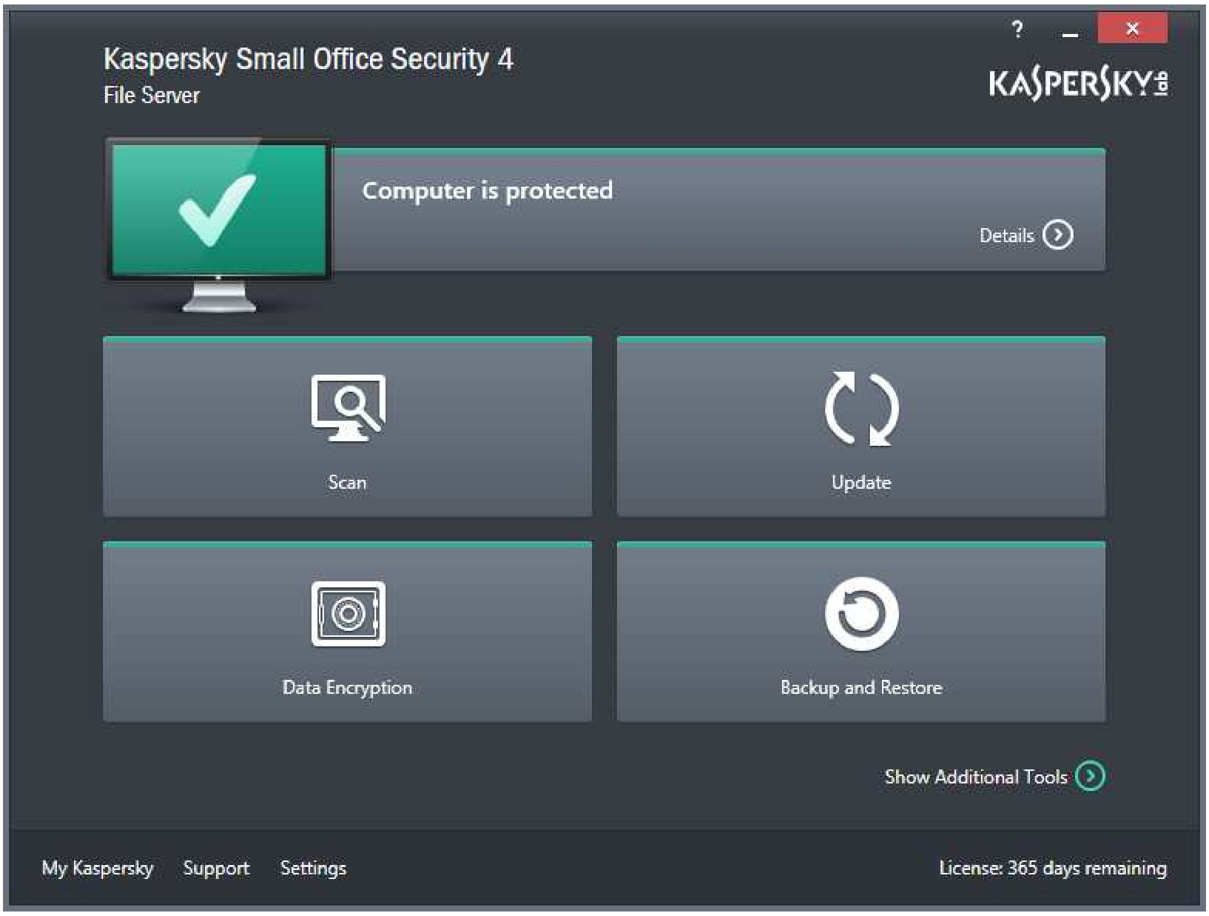


Malicious web page Firefox threatens the security of your computer

Web page: http://www.eicar.org/download/eicar.com
We recommend that you close the web page.

Details

## Windows server protection software



Kaspersky Small Office Security 4

File Server

Computer is protected

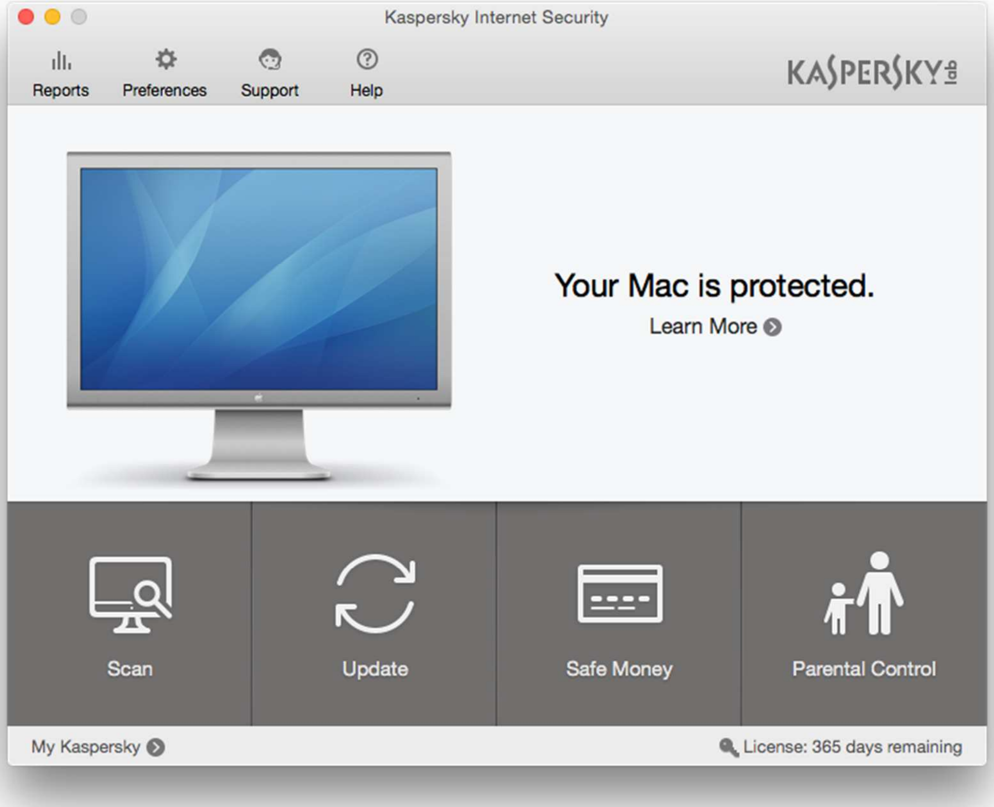
License: 365 days remaining

The *File Server* variant of the KSOS windows protection software is very similar to the *Personal Computer* software. There are fewer features, and some configuration differences, but basic functionality is identical.

### Comment

We found the Windows protection software to be very well designed, with a clear status display and malware warnings, easy rectification of any problems, and all essential information and features easily accessible from the home page.

## Mac client protection software



Your Mac is protected.

Learn More

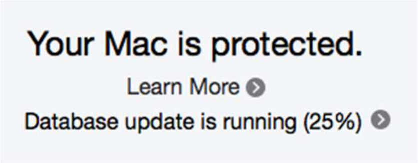
License: 365 days remaining

### Installation

The .DMG installer file downloaded from the console can be double-clicked to start; the administrator then only has to click *Install…* and decide whether to participate in the Kaspersky Security Network, then click *Download and install*. No further interaction is required.

### Main program window

This features a very prominent status display, with the essential functions scan, update, help, settings and licence information all easily accessible from the home page. The status display shows the progress of updates:

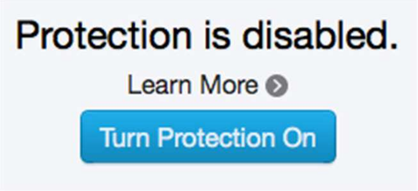


Your Mac is protected.

Learn More

Database update is running (25%)

It also shows a warning if protection is disabled, and displays a button with which it can instantly be re-enabled:

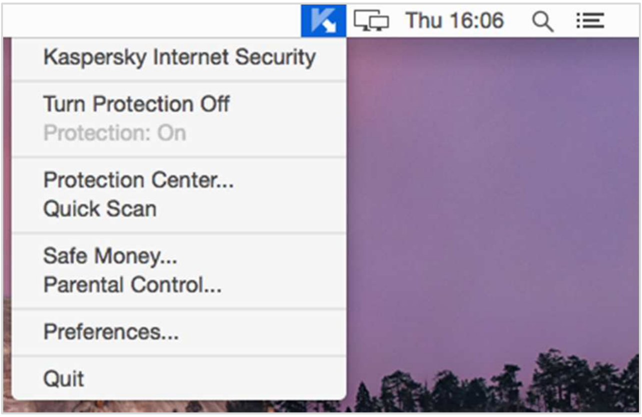


Protection is disabled.

Learn More

## System Tray icon

KSOS displays an icon in the OS X System Tray, which shows a menu of common tasks:

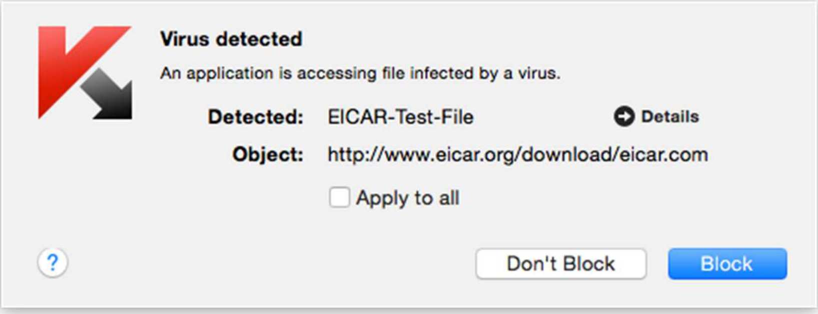


## Unauthorised access

The protection features can only be configured by entering administrator credentials for Mac OS X, preventing standard users from disabling them.

## Malware alerts

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



**Virus detected**

An application is accessing file infected by a virus.

**Detected:** EICAR-Test-File

**Object:** http://www.eicar.org/download/eicar.com

□ Apply to all

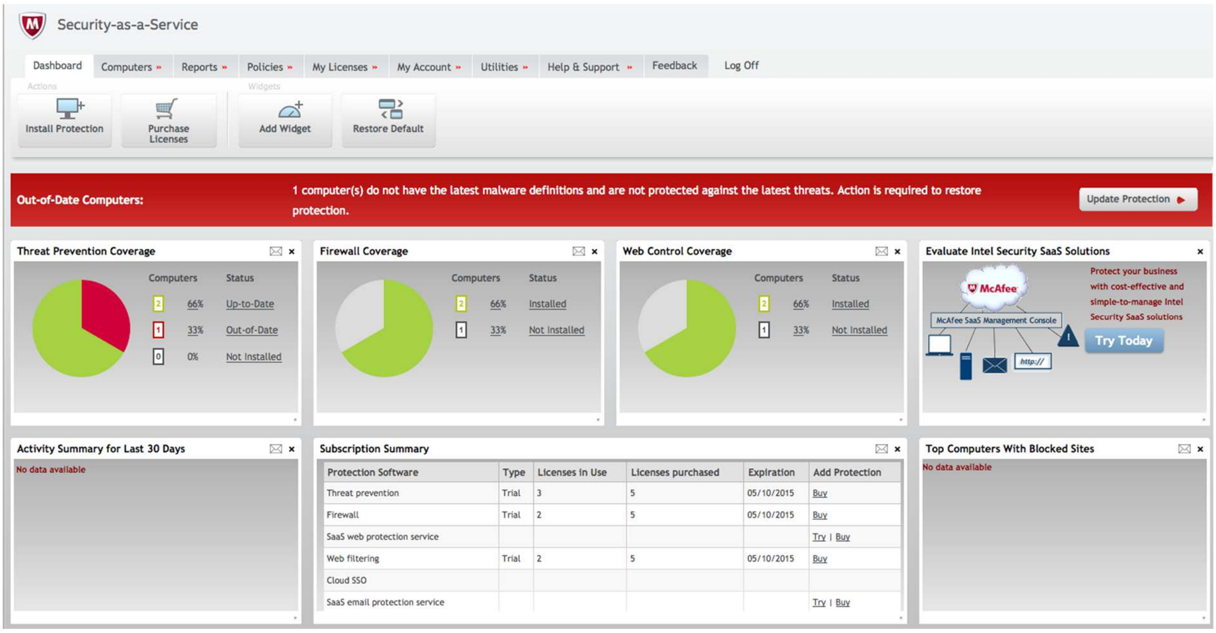
## Comment

We feel the Mac client software will prove very easy to use. There is a clear status display, which warns in the event of a problem and makes this easy to rectify. All the essential functions are easy to find in the program's home page.

## Summary

We feel that Kaspersky Small Office Security 4 is exceptionally well-suited to a small-business network without professional IT support. Deploying and managing the protection software from the console should be a straightforward task for anyone who can install and use iTunes. The product is a very obvious choice for small companies who want centrally managed, professional security software for a Windows server, plus Windows and Mac desktops and laptops and Android Phone/Tablets, without having to employ dedicated IT staff to look after it.

# McAfee SaaS Endpoint Protection



Out-of-Date Computers: 1 computer(s) do not have the latest malware definitions and are not protected against the latest threats. Action is required to restore protection.

Threat Prevention Coverage

| Computers | | Status |
|---|---|---|
| 2 | 66% | Up-to-Date |
| 1 | 33% | Out-of-Date |
| 0 | 0% | Not Installed |

Firewall Coverage

| Computers | | Status |
|---|---|---|
| 2 | 66% | Installed |
| 1 | 33% | Not Installed |

Web Control Coverage

| Computers | | Status |
|---|---|---|
| 2 | 66% | Installed |
| 1 | 33% | Not Installed |

Evaluate Intel Security SaaS Solutions

Protect your business with cost-effective and simple-to-manage Intel Security SaaS solutions

Activity Summary for Last 30 Days

No data available

Subscription Summary

| Protection Software | Type | Licenses in Use | Licenses purchased | Expiration | Add Protection |
|---|---|---|---|---|---|
| Threat prevention | Trial | 3 | 5 | 05/10/2015 | Buy |
| Firewall | Trial | 2 | 5 | 05/10/2015 | Buy |
| SaaS web protection service | | | | | Try \| Buy |
| Web filtering | Trial | 2 | 5 | 05/10/2015 | Buy |
| Cloud SSO | | | | | |
| SaaS email protection service | | | | | Try \| Buy |

Top Computers With Blocked Sites

No data available

## Introduction

McAfee make a wide range of security products for businesses large and small. We have reviewed McAfee SaaS Endpoint Protection, which uses a cloud-based console to manage clients.

## Software versions reviewed

McAfee SaaS cloud console as at 5th September 2015
McAfee Endpoint Security client for Windows 10.0.1

## Supported operating systems

Windows clients: Windows XP, Vista, 7, 8.

Windows servers: Windows Server 2003, 2008/R2, 2012; Windows Small Business Server 2003/R2, 2008, 2011.

## Documentation

### Manuals

The *Help & Support* menu at the top of the console includes links to the Installation Guide and Guide to SaaS Endpoint Protection. The former is a 43-page document with instructions for deploying the client protection software. Whilst it has been well produced and the instructions are clear, we would say that it is aimed more at experienced administrators than non-experts, and there are no screenshots. The Guide to SaaS Endpoint Protection is a very detailed and comprehensive manual of 181 pages. Again we would say that this is oriented towards experienced IT professionals rather than small-business owners.

### Knowledge base

The McAfee Knowledge Center is a searchable online database of support articles. As with the manuals, we feel this is aimed at experienced IT professionals.

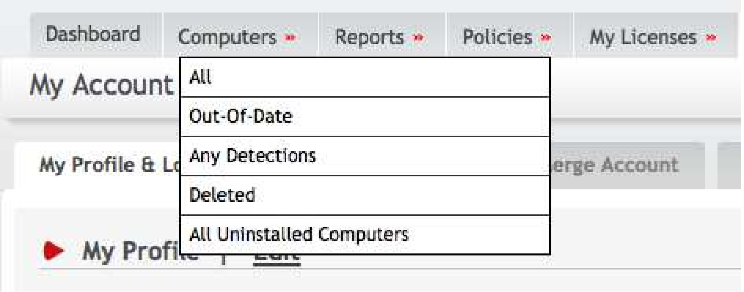
## Management Console

### Installation and configuration

The console is cloud-based, so no installation or configuration is necessary; the administrator simply opens the URL in a browser and logs in.

### Layout

The console opens by default on the *Dashboard* page. This displays a number of panels, each with an element of status or activity information, such as individual protection components, subscription information, malware detection and web-filtering data. This area is very customisable; the admin can move panels around by drag and drop, remove individual panels by clicking the *x* in the corner, or add additional panels by clicking *Add Widget* on the toolbar at the top. A row of tabs along the top of the console allows the admin to change to other pages, such as *Computers, Reports, Policies, My Licences, My Account, Utilities, Help and Support*. Each tab has a double function; the admin can simply click it to go to the associated page, or hover the mouse over it, in which case a menu of more specific options is shown. The screenshot below shows that the *Computers* tab, which if clicked displays all computers on the network, can also be used to show only specific types of computer by hovering:

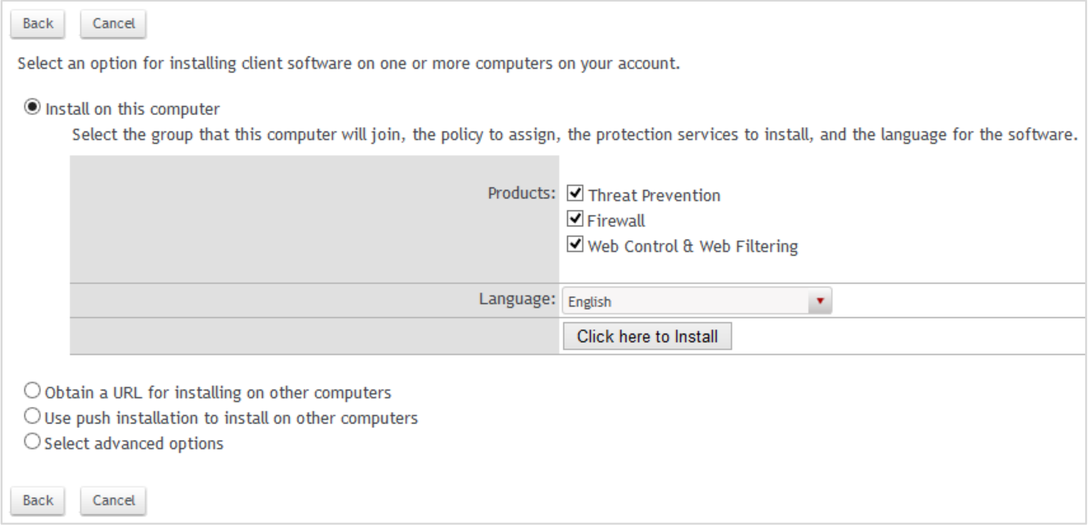


### Preparing devices for deployment

We did not have to make any preparation of client or server computers before deploying the protection software.

### Deploying the endpoint protection software

To deploy the protection software, the admin clicks on Install Protection in the top left-hand corner of the Dashboard. This takes the admin to the installation page, which includes options for local installation, push installation, and obtaining a URL which can be emailed to users:



Select an option for installing client software on one or more computers on your account.

● Install on this computer

Select the group that this computer will join, the policy to assign, the protection services to install, and the language for the software.

Products: ☑ Threat Prevention ☑ Firewall ☑ Web Control & Web Filtering

Language: English

○ Obtain a URL for installing on other computers

○ Use push installation to install on other computers

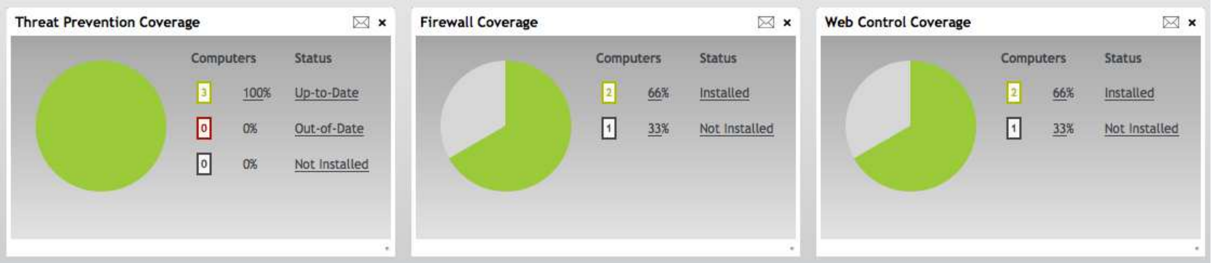
○ Select advanced options

We chose to use the default option of 'Install on this computer' for the purposes of this review.

## Monitoring the network

### *Status*

For each of the main protection components *Threat Prevention, Firewall* and *Web Control*, there is a panel on the dashboard, with a pie chart showing clearly what percentage of clients have the product running:



Threat Prevention Coverage

| Computers | | Status |
|---|---|---|
| 3 | 100% | Up-to-Date |
| 0 | 0% | Out-of-Date |
| 0 | 0% | Not Installed |

Firewall Coverage

| Computers | | Status |
|---|---|---|
| 2 | 66% | Installed |
| 1 | 33% | Not Installed |

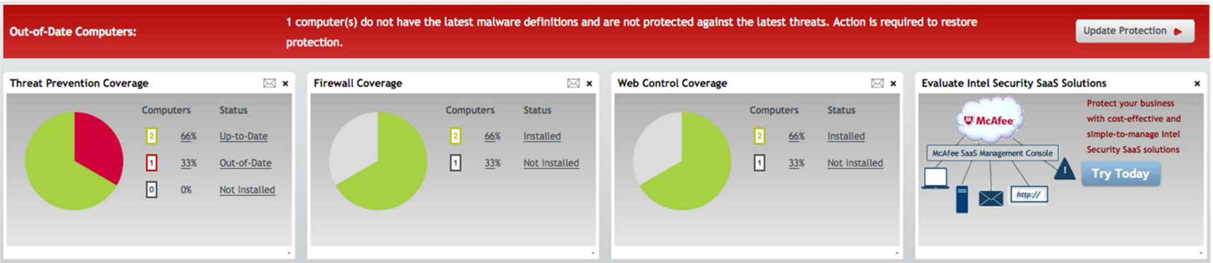
Web Control Coverage

| Computers | | Status |
|---|---|---|
| 2 | 66% | Installed |
| 1 | 33% | Not Installed |

We note that the *Threat Prevention Coverage* panel shows whether the component is installed and up to date, but not whether real-time protection is enabled.

### *Warnings and rectifying problems*

The screenshot below illustrates the warnings shown if a client's malware signatures are out of date. The pie chart for *Threat Protection Coverage* shows a third of PCs (one out of our three test clients) in red, as opposed to green for up to date; additionally, a red strip along the top of the console warns explicitly of the problem:



Out-of-Date Computers: 1 computer(s) do not have the latest malware definitions and are not protected against the latest threats. Action is required to restore protection.

Threat Prevention Coverage

| Computers | | Status |
|---|---|---|
| 2 | 66% | Up-to-Date |
| 1 | 33% | Out-of-Date |
| 0 | 0% | Not Installed |

Firewall Coverage

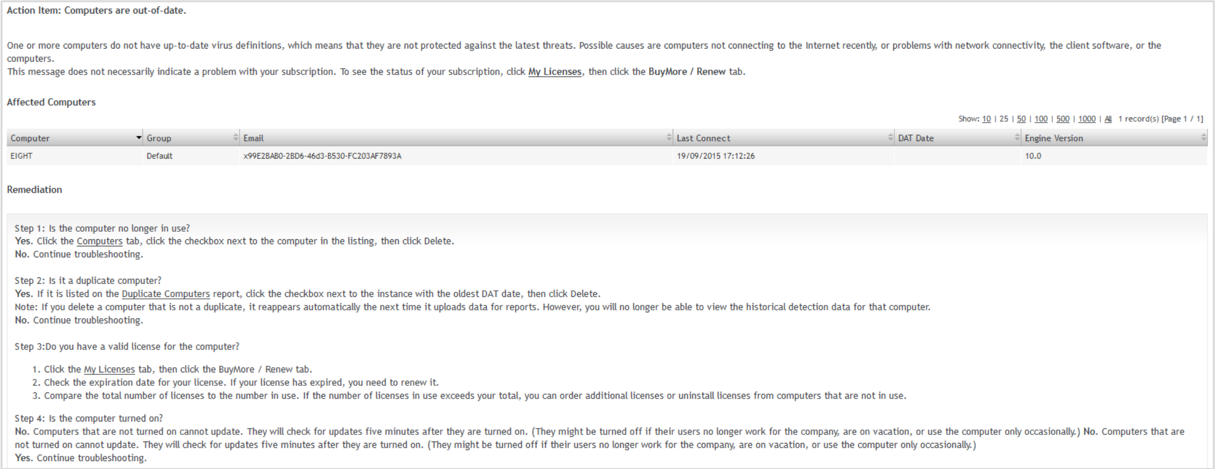
| Computers | | Status |
|---|---|---|
| 2 | 66% | Installed |
| 1 | 33% | Not Installed |

Web Control Coverage

| Computers | | Status |
|---|---|---|
| 2 | 66% | Installed |
| 1 | 33% | Not Installed |

Evaluate Intel Security SaaS Solutions
McAfee
McAfee SaaS Management Console
http://
Protect your business with cost-effective and simple-to-manage Intel Security SaaS solutions
Try Today

An *Update Protection* button is displayed; clicking this opens a very detailed help page, which explains possible reasons why the protection might be out of date (including the computer being switched off because the user is on holiday), and the appropriate course of action to take in each case:



**Action Item: Computers are out-of-date.**

One or more computers do not have up-to-date virus definitions, which means that they are not protected against the latest threats. Possible causes are computers not connecting to the Internet recently, or problems with network connectivity, the client software, or the computers.
This message does not necessarily indicate a problem with your subscription. To see the status of your subscription, click My Licenses, then click the **BuyMore / Renew** tab.

**Affected Computers**

Show: 10 | 25 | 50 | 100 | 500 | 1000 | All 1 record(s) [Page 1 / 1]

| Computer | Group | Email | Last Connect | DAT Date | Engine Version |
|---|---|---|---|---|---|
| EIGHT | Default | x99E2BAB0-2BD6-46d3-B530-FC203AF7893A | 19/09/2015 17:12:26 | | 10.0 |

**Remediation**

Step 1: Is the computer no longer in use?
**Yes.** Click the Computers tab, click the checkbox next to the computer in the listing, then click Delete.
**No.** Continue troubleshooting.

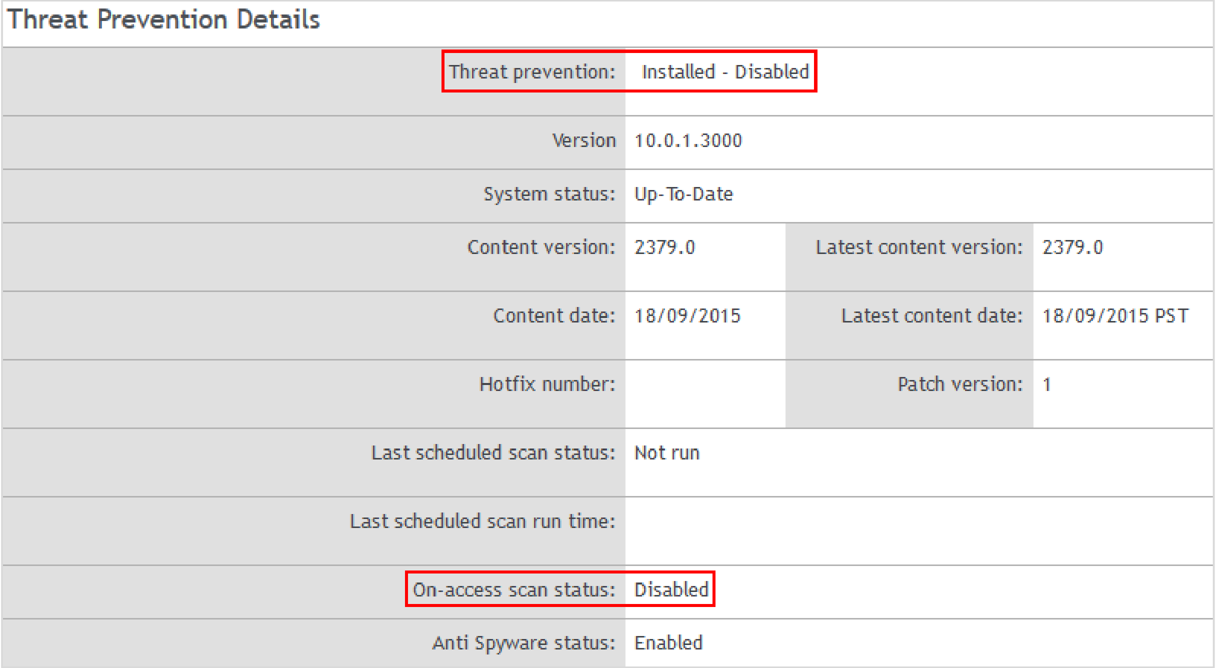
Step 2: Is it a duplicate computer?
**Yes.** If it is listed on the Duplicate Computers report, click the checkbox next to the instance with the oldest DAT date, then click Delete.
Note: If you delete a computer that is not a duplicate, it reappears automatically the next time it uploads data for reports. However, you will no longer be able to view the historical detection data for that computer.
**No.** Continue troubleshooting.

Step 3:Do you have a valid license for the computer?

1. Click the My Licenses tab, then click the BuyMore / Renew tab.
2. Check the expiration date for your license. If your license has expired, you need to renew it.
3. Compare the total number of licenses to the number in use. If the number of licenses in use exceeds your total, you can order additional licenses or uninstall licenses from computers that are not in use.

Step 4: Is the computer turned on?
**No.** Computers that are not turned on cannot update. They will check for updates five minutes after they are turned on. (They might be turned off if their users no longer work for the company, are on vacation, or use the computer only occasionally.) **No.** Computers that are not turned on cannot update. They will check for updates five minutes after they are turned on. (They might be turned off if their users no longer work for the company, are on vacation, or use the computer only occasionally.)
**Yes.** Continue troubleshooting.

In our test, we found that if real-time protection is disabled on a client, no obvious warning is shown in the console, even though the component's status will be shown as *Disabled* in the details page of the computer affected:



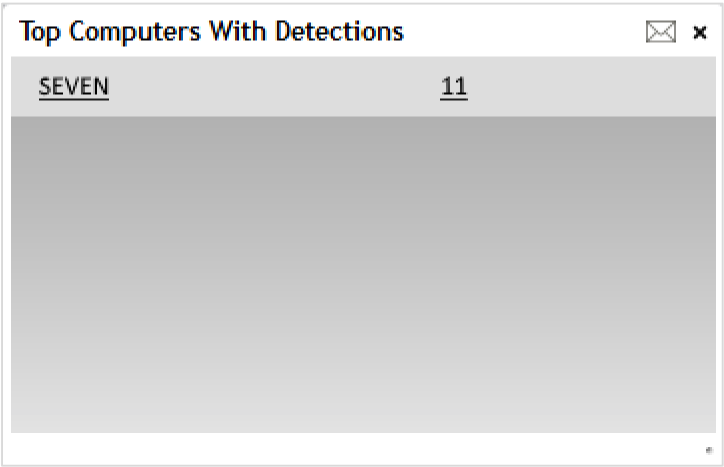
Threat Prevention Details

| | | | |
|---|---|---|---|
| Threat prevention: | Installed - Disabled | | |
| Version | 10.0.1.3000 | | |
| System status: | Up-To-Date | | |
| Content version: | 2379.0 | Latest content version: | 2379.0 |
| Content date: | 18/09/2015 | Latest content date: | 18/09/2015 PST |
| Hotfix number: | | Patch version: | 1 |
| Last scheduled scan status: | Not run | | |
| Last scheduled scan run time: | | | |
| On-access scan status: | Disabled | | |
| Anti Spyware status: | Enabled | | |

McAfee makes use of the Microsoft Security Center to alert the user, and it is also possible via the console to have an email automatically sent to the administrator on a daily and/or monthly basis, showing that a component has entered a disabled state. However, this is not ideal in our view, and we would prefer an 'alert' banner and 'fix' button that is similar to the 'out of date' alerts that exist in the console, to make it more obvious that all is not well.

### *Malware alerts*

Computers on which malware has been detected are shown in the *Top Computers With Detections* panel in the *Dashboard*. Additionally, using the *Any Detections* filter of the *Computers* page will show computers with detections.



Top Computers With Detections

| | |
|---|---|
| SEVEN | 11 |

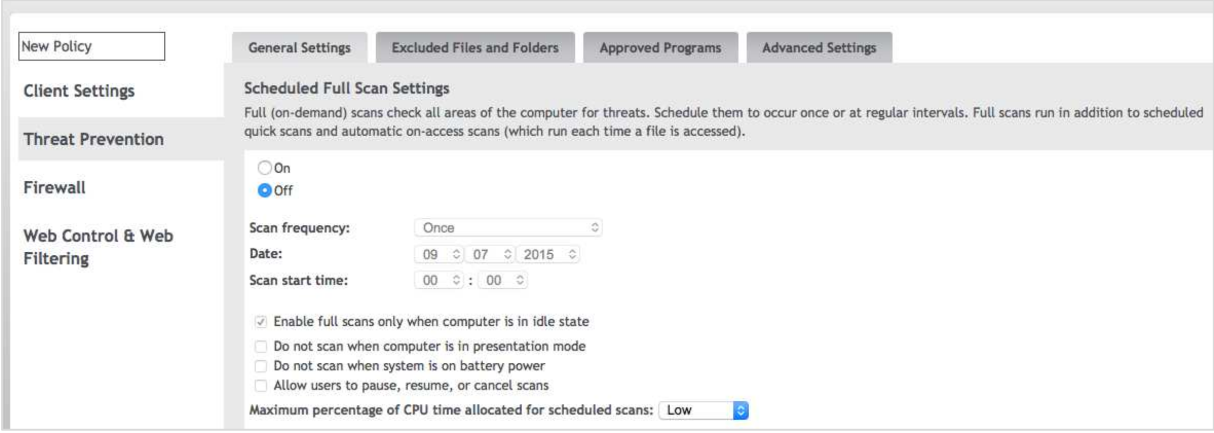
### *Program version*

The administrator can find the version number of the endpoint software on an individual client by going to the *Computers* page and clicking the name of the client PC; this displays detailed system information, including OS details, IP address, status of components, and details of malware signatures, in addition to the program version.

## Managing the network

### *Scanning*

Scans can be run by policy, by clicking the *Policies* tab, *Threat Prevention*. The admin can choose a full or quick scan, when to run the scan, and various other options (scan configuration page shown below).



Scheduled Full Scan Settings

Full (on-demand) scans check all areas of the computer for threats. Schedule them to occur once or at regular intervals. Full scans run in addition to scheduled quick scans and automatic on-access scans (which run each time a file is accessed).

○ On
● Off

Scan frequency: Once
Date: 09 07 2015
Scan start time: 00 : 00

☑ Enable full scans only when computer is in idle state
☐ Do not scan when computer is in presentation mode
☐ Do not scan when system is on battery power
☐ Allow users to pause, resume, or cancel scans

Maximum percentage of CPU time allocated for scheduled scans: Low

### *Scheduled scans*

These are set up using exactly the same way as one-off scans, by clicking the *Scan frequency* drop-down list, and choosing *Daily, Weekly, Monthly* or *Run on next policy update*.

### *Updates*

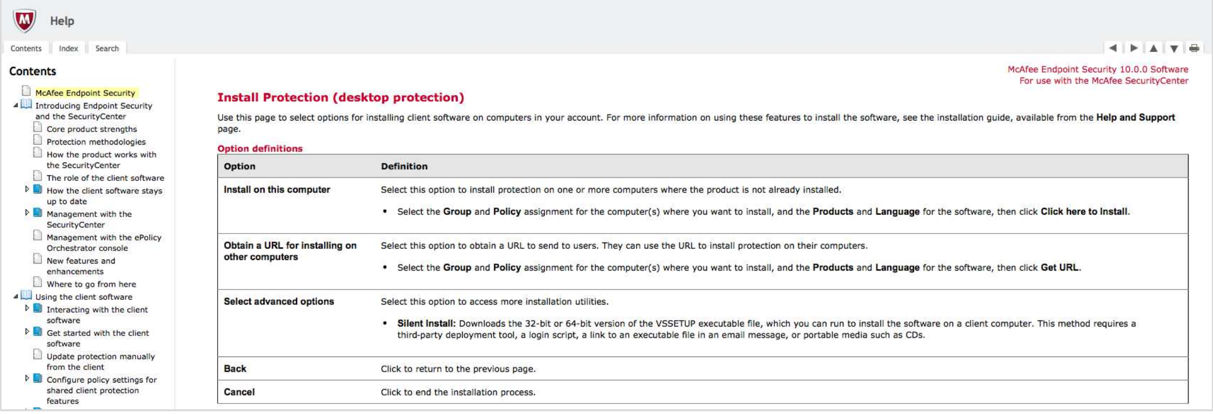
Updates are scheduled by default to run every 12 hours; the policy can be configured to change this to every 4, 8, 16 or 24 hours. A manual update can only be run locally on the client endpoint software.

### *Removing devices from the console*

To remove a computer from the console, the admin selects the relevant check box on the *Computers* page and clicks the *Delete* button above.

### Integrated help feature

Clicking the *?* symbol in the top right-hand corner of the console opens the product's online help feature. This is context-sensitive, i.e. opens at the relevant page for the console feature currently being used. It provides a comprehensive list of topics in a left-hand panel, with details for the selected topic shown in the main panel. We found the instructions to be clearly written, although unfortunately with very few screenshots.


Help
Contents
Index
Search
Contents
McAfee Endpoint Security
Introducing Endpoint Security and the SecurityCenter
Core product strengths
Protection methodologies
How the product works with the SecurityCenter
The role of the client software
How the client software stays up to date
Management with the SecurityCenter
Management with the ePolicy Orchestrator console
New features and enhancements
Where to go from here
Using the client software
Interacting with the client software
Get started with the client software
Update protection manually from the client
Configure policy settings for shared client protection features

McAfee Endpoint Security 10.0.0 Software
For use with the McAfee SecurityCenter

**Install Protection (desktop protection)**

Use this page to select options for installing client software on computers in your account. For more information on using these features to install the software, see the installation guide, available from the **Help and Support** page.

**Option definitions**

| Option | Definition |
|---|---|
| **Install on this computer** | Select this option to install protection on one or more computers where the product is not already installed.<br>• Select the **Group** and **Policy** assignment for the computer(s) where you want to install, and the **Products** and **Language** for the software, then click **Click here to Install**. |
| **Obtain a URL for installing on other computers** | Select this option to obtain a URL to send to users. They can use the URL to install protection on their computers.<br>• Select the **Group** and **Policy** assignment for the computer(s) where you want to install, and the **Products** and **Language** for the software, then click **Get URL**. |
| **Select advanced options** | Select this option to access more installation utilities.<br>• **Silent Install:** Downloads the 32-bit or 64-bit version of the VSSETUP executable file, which you can run to install the software on a client computer. This method requires a third-party deployment tool, a login script, a link to an executable file in an email message, or portable media such as CDs. |
| **Back** | Click to return to the previous page. |
| **Cancel** | Click to end the installation process. |

## Comment

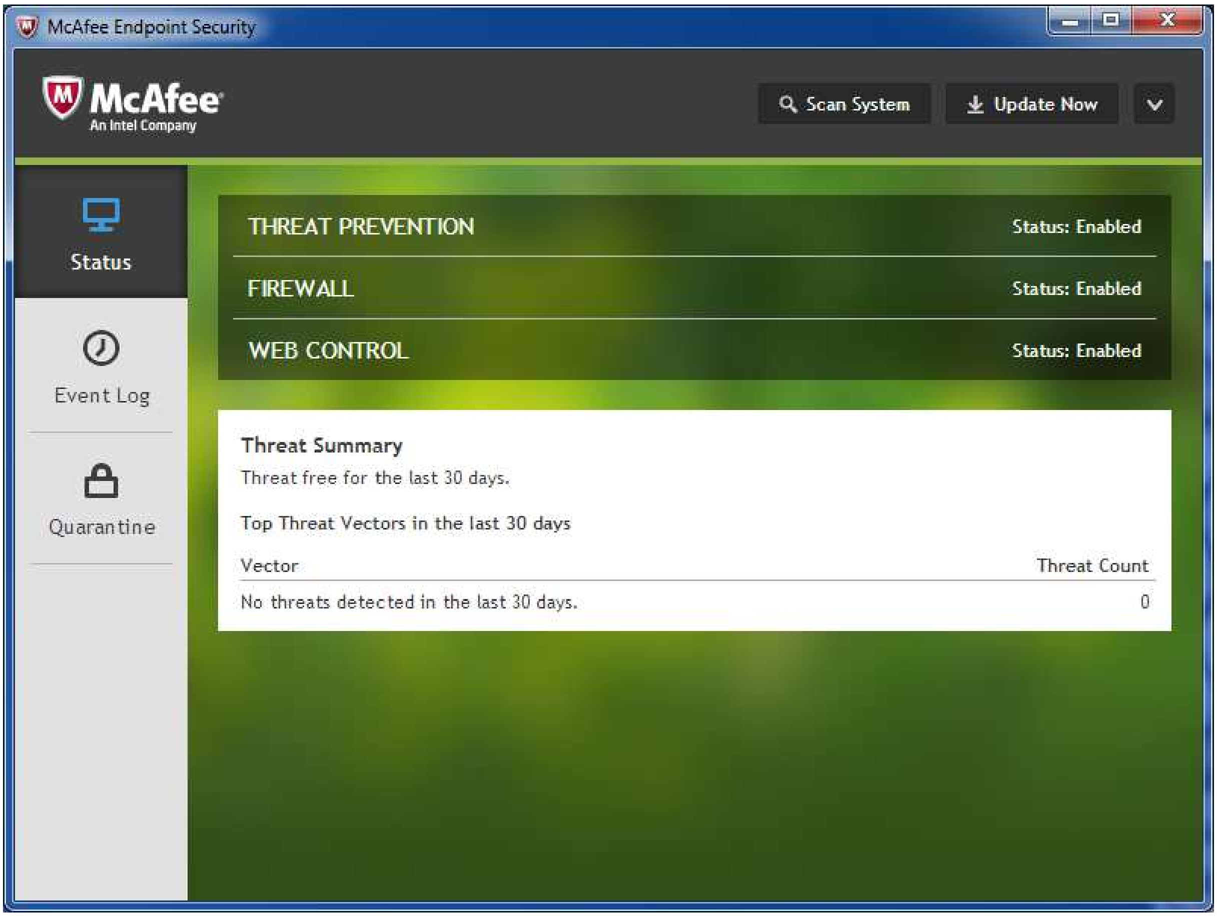
We feel the *Dashboard* page of the console does a very good job of displaying a clear overview of important information, and we particularly liked the ability to customise it so easily, so each admin can add or remove panels and arrange them as he/she sees fit. We also feel the single row of tabs along the top of the console makes it very easy to navigate between pages, and the click-or-hover option with each tab is innovative and useful. The pages all provide a clear overview of the available functions, without overwhelming the admin.

Whilst running a scan by means of a policy will be very familiar to IT professionals used to enterprise consoles, we feel it will probably be a new concept to inexperienced admins using a management console for the first time. Simultaneously re-applying the protection policy every time an update runs strikes us as very sensible, although we would prefer to see a shorter update interval (4 hours is the minimum) available.

We liked the very obvious alert shown by the console when a client's malware signatures are out of date, and the convenient link to possible solutions. We feel it would be a valuable addition if a similar warning and "fix" button were displayed when real-time protection is disabled.

The integrated help feature is extensive, and probably the best source of information for inexperienced admins. We were impressed with the information page that explains possible reasons a computer might be out of date, and feel it would be educational for inexperienced admins.

## Windows client protection software



THREAT PREVENTION Status: Enabled

FIREWALL Status: Enabled

WEB CONTROL Status: Enabled

Threat Summary

Threat free for the last 30 days.

Top Threat Vectors in the last 30 days

| Vector | Threat Count |
|---|---|
| No threats detected in the last 30 days. | 0 |

### Installation

We chose the local installation option, i.e. downloading the installer file from the console and running it on the same computer. The screenshot in the *Deploying the endpoint protection software* in the *Management* section above shows the component and language options, which are selected before the installer is downloaded. Once the setup file has been started, no further interaction is required from the administrator.

### Main program window

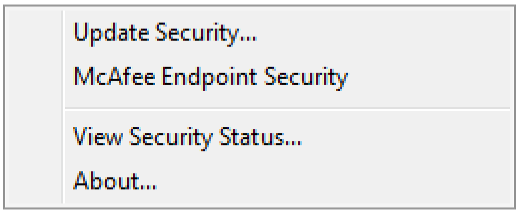
This includes a status display for individual protection components, scan and update buttons, and a single menu from which the help and support functions can be accessed. If either the *Firewall* or *Web Control* component is deactivated, the relevant status box will show the component status as *Disabled*. With *Threat Protection*, which has four sub-components, the overall status is only shown as *Disabled* if all four of these are deactivated.

### Windows Security Center/Windows Defender

Assuming the default installation (all components) has been selected, McAfee Endpoint Protection registers as firewall, antivirus and antispyware. Under Windows 7, Windows Defender is disabled.

### System Tray icon

A System Tray icon is installed, which can be used to display the following menu:



Update Security...
McAfee Endpoint Security

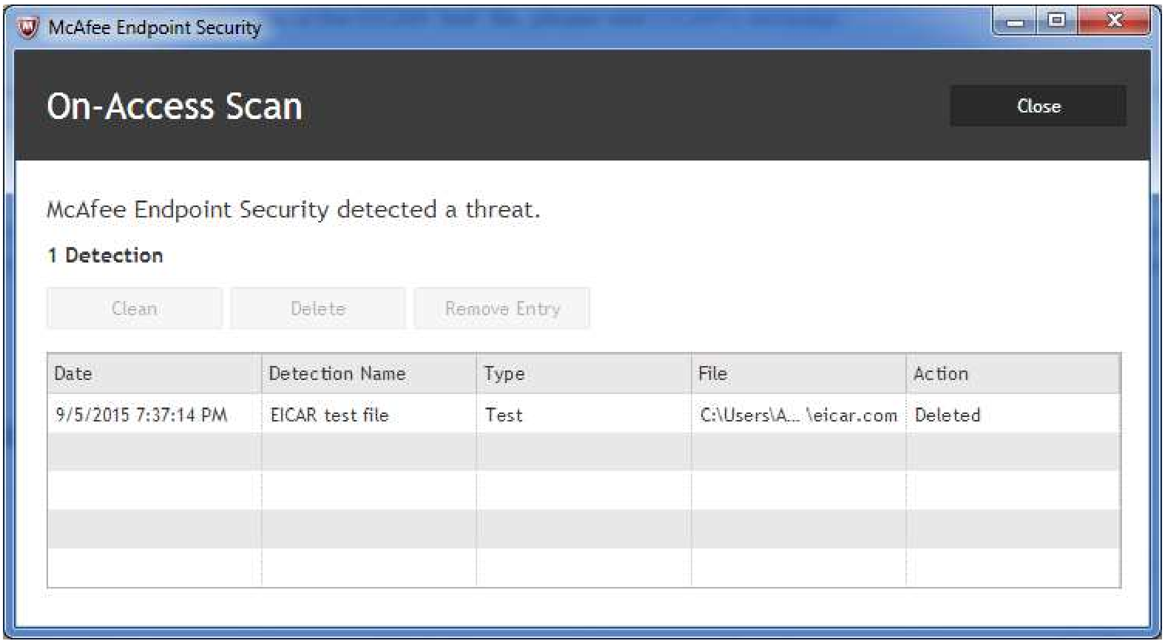
View Security Status...
About...

### Unauthorised access

By default, protection components can be disabled from standard user accounts. This can be prevented by configuring *Standard Access* rather than the default *Full Access*, whereby a password has to be entered before settings can be changed. The administrator can do this locally on the client software of each PC, or apply a policy to individual PCs, groups of PCs, or all PCs from the management console. We would strongly advise admins to do this.

### Malware alerts

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



McAfee Endpoint Security

On-Access Scan

McAfee Endpoint Security detected a threat.

1 Detection

| Date | Detection Name | Type | File | Action |
|---|---|---|---|---|
| 9/5/2015 7:37:14 PM | EICAR test file | Test | C:\Users\A... \eicar.com | Deleted |

## Windows server protection software

This can be regarded as identical to the Windows client software.

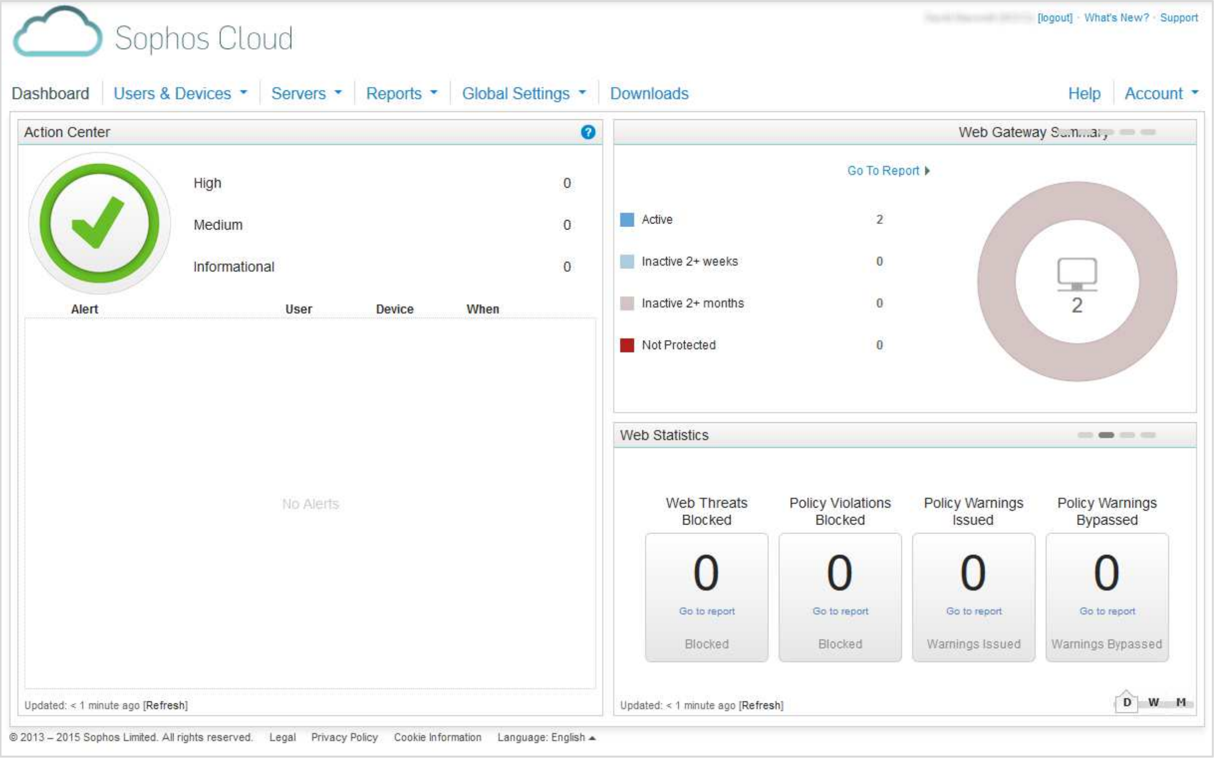
### Comment

We feel the design of the Windows client/server protection software is very familiar and easy to use, enabling users to run scans and updates. Installation is very straightforward, and provides useful component and language options.

## Summary

We found McAfee SaaS Endpoint Protection to be well suited to small businesses without full-time IT support. The console is cloud-based and so requires no installation, provides a clear overview of important information and tasks, automated email-based reporting, and is straightforward to find one’s way around. There is a very usable integrated help feature too. The client software has a familiar layout and is easy to use. We have one suggestion for improvement: we feel it would be a valuable addition if the very clear warning and convenient “fix” button shown for out-of-date computers were extended so that they also cover ‘disabled’ firewall/real-time protection.

# Sophos Cloud


Sophos Cloud
[redacted] [logout] · What's New? · Support
Dashboard
Users & Devices
Servers
Reports
Global Settings
Downloads
Help
Account
Action Center
Web Gateway Summary
Go To Report
2
Web Statistics
D W M
© 2013 – 2015 Sophos Limited. All rights reserved. Legal Privacy Policy Cookie Information Language: English

| | |
|---|---|
| High | 0 |
| Medium | 0 |
| Informational | 0 |

| Alert | User | Device | When |
|---|---|---|---|

No Alerts

Updated: < 1 minute ago [Refresh]

| | |
|---|---|
| Active | 2 |
| Inactive 2+ weeks | 0 |
| Inactive 2+ months | 0 |
| Not Protected | 0 |

| Web Threats Blocked | Policy Violations Blocked | Policy Warnings Issued | Policy Warnings Bypassed |
|---|---|---|---|
| 0<br>Go to report<br>Blocked | 0<br>Go to report<br>Blocked | 0<br>Go to report<br>Warnings Issued | 0<br>Go to report<br>Warnings Bypassed |

Updated: < 1 minute ago [Refresh]

## Introduction

Sophos specialises in security software for business, and makes a wide range of products. Sophos Cloud uses a cloud-based console to manage protection software for clients.

## Software versions reviewed

Sophos Endpoint Security and Control (ESC) for Workstations 11.1.2 Cloud
Sophos ESC for Windows Servers 1.1.7 Cloud Server
Sophos Cloud Endpoint for Mac 9.3.3

## Supported operating systems

Windows XP, Vista, 7, 8, 8.1, 10
Windows Server 2003/R2, 2008/R2, 2012/R2
Windows Small Business Server 2011
Mac OS X 10.6,10.7,10.8,10.9,10.10
Linux[13]
Android/iOS: please see feature list

## Documentation

### Manuals

A 91-page manual in .PDF format is available; it can be downloaded from the Help window, as described above. It is comprehensive, and easily navigable thanks to a clickable contents page and bookmarks. We found the text to be well written, although unfortunately there are no screenshots.

[13] https://www.sophos.com/en-us/support/knowledgebase/118624.aspx

### Knowledge base

An FAQ page and knowledge base are provided; the latter can be searched for instructions for specific tasks.

### Comment

We found Sophos' documentation to be good.

## Management Console

### Installation and configuration

The console is cloud-based and so does not require installation. The administrator simply creates an account, opens the URL, and logs in.

### Layout

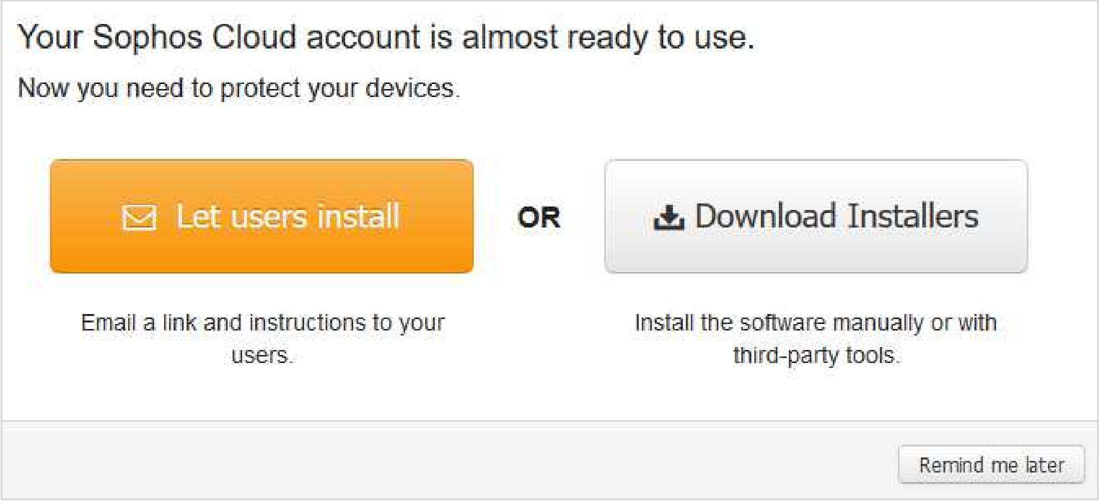
The home page of the console consists of one large panel showing overall security status, along with two smaller panels that each display a "slideshow" of different content. Items shown include resolved malware detections, global malware activity, and summaries of activity relating to servers, computers, and mobile devices.

### Preparing devices for deployment

We did not need to make any preparations to client or server systems before installing the protection software.

### Deploying the endpoint protection software

When the admin first logs into the console, the following deployment options are displayed:



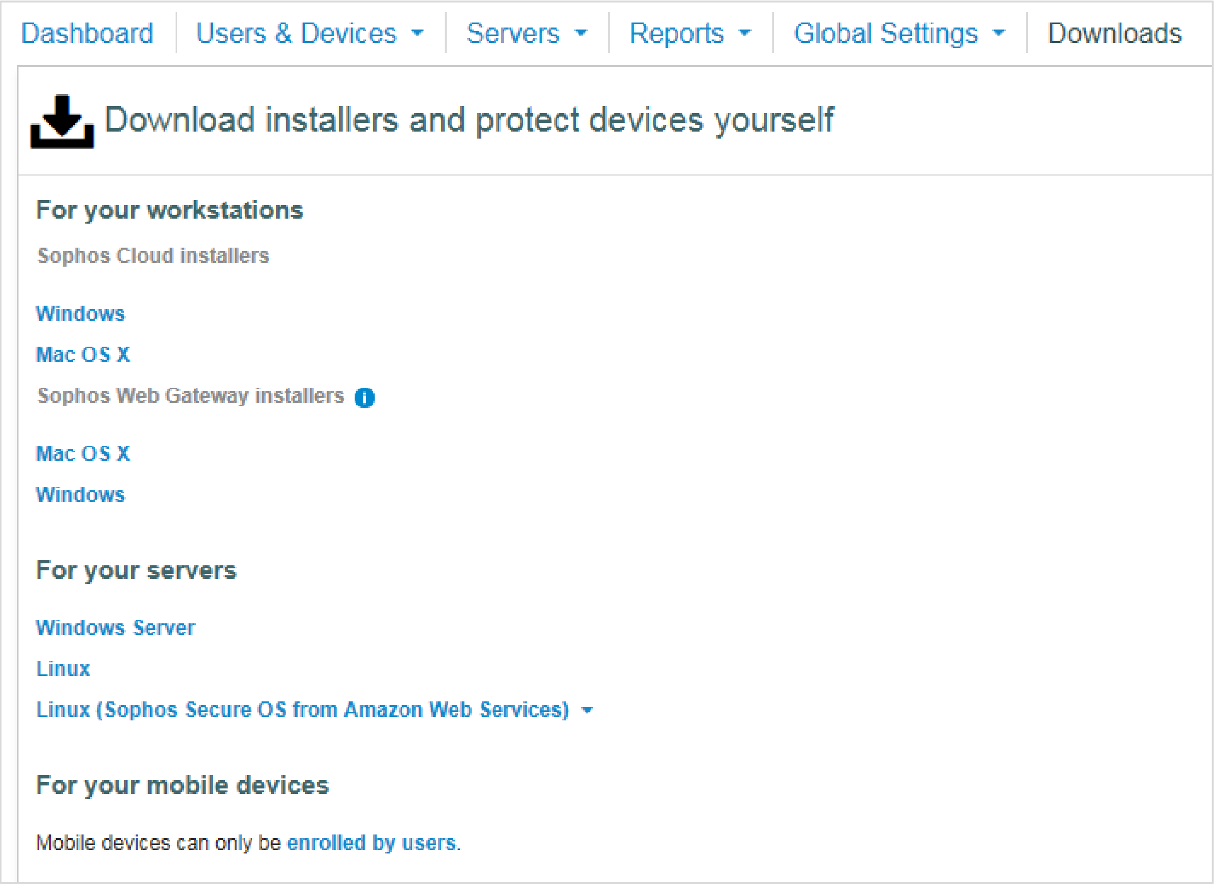
Your Sophos Cloud account is almost ready to use.

Now you need to protect your devices.

Email a link and instructions to your users.

Install the software manually or with third-party tools.

We opted for the *Download Installers* method; this takes the admin to the *Downloads* page of the console, where the protection software can be downloaded:



Download installers and protect devices yourself

For your workstations

Sophos Cloud installers

Windows

Mac OS X

Sophos Web Gateway installers

Mac OS X

Windows

For your servers

Windows Server

Linux

Linux (Sophos Secure OS from Amazon Web Services)

For your mobile devices

Mobile devices can only be enrolled by users.

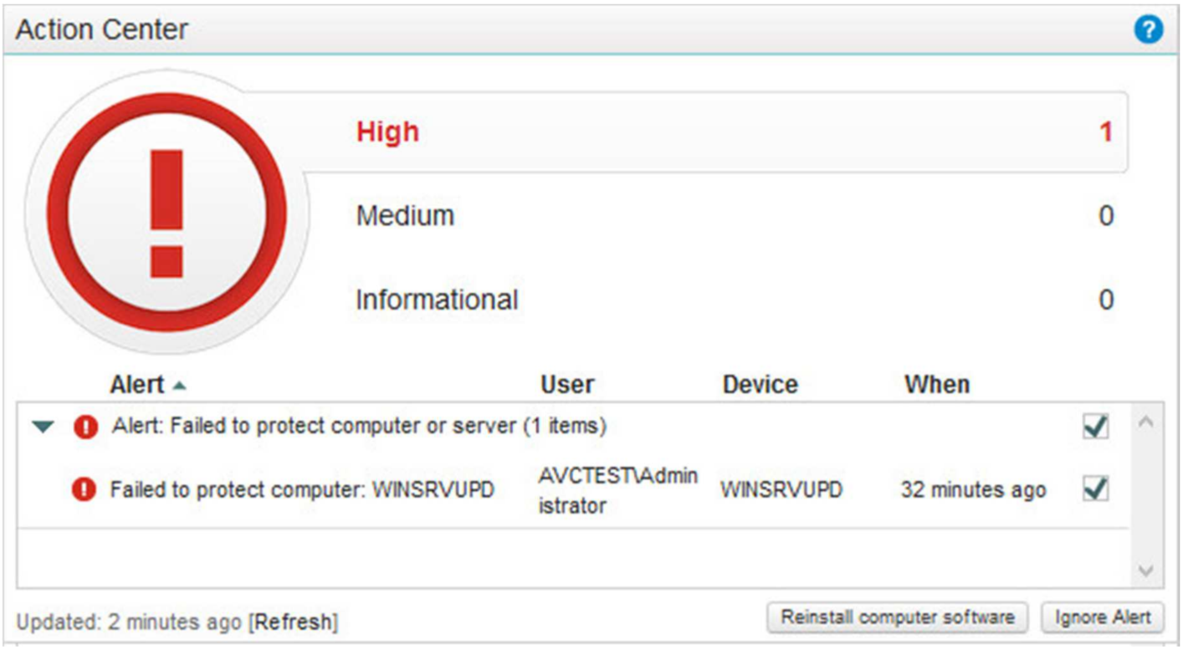
## Monitoring the network

### *Status*

The *Action Center*, the status panel on the home page, shows the number of devices with problems. If all is well, a big green tick (checkmark) symbol is displayed.

### *Warnings and rectifying problems*

In the event of an installation failing, the *Alerts* panel in the *Action Center* shows clearly what is wrong:


Action Center

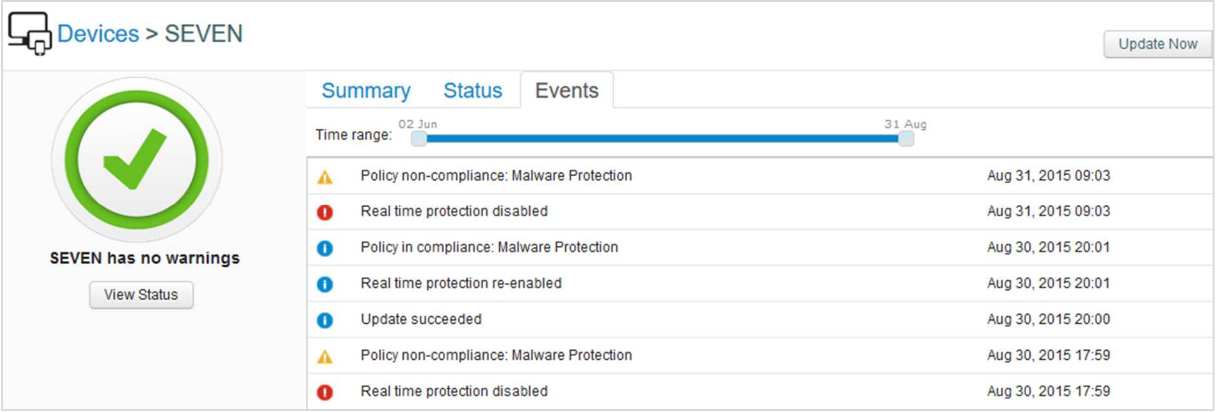
| | |
|---|---|
| High | 1 |
| Medium | 0 |
| Informational | 0 |

| Alert ▲ | User | Device | When | |
|---|---|---|---|---|
| Alert: Failed to protect computer or server (1 items) | | | | ☑ |
| Failed to protect computer: WINSRVUPD | AVCTEST\Administrator | WINSRVUPD | 32 minutes ago | ☑ |

Updated: 2 minutes ago [Refresh]

The screenshot above shows the convenient solution provided for the problem, namely the *Reinstall computer software* button.

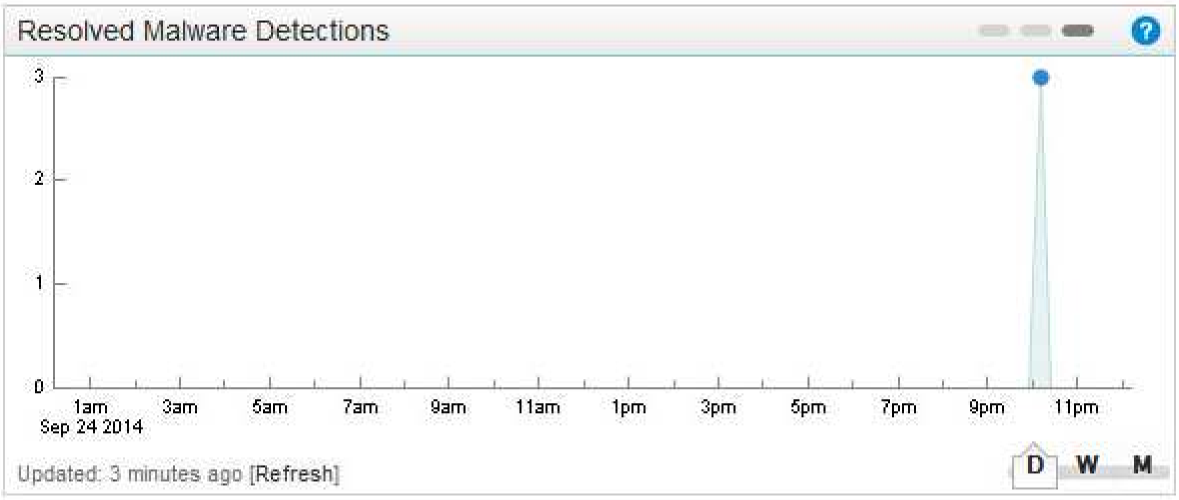
In our test, we found that if real-time protection is disabled on a client device, or if the endpoint protection software is uninstalled locally, the system will automatically fix the problem. The screenshot below shows that RTP was disabled at 17:59 on August 30th, and reactivated at 20:01; likewise, when we uninstalled the endpoint software from the client, we found that it was reinstalled 2 hours later.



| | | |
|---|---|---|
| ⚠ | Policy non-compliance: Malware Protection | Aug 31, 2015 09:03 |
| ❗ | Real time protection disabled | Aug 31, 2015 09:03 |
| ⓘ | Policy in compliance: Malware Protection | Aug 30, 2015 20:01 |
| ⓘ | Real time protection re-enabled | Aug 30, 2015 20:01 |
| ⓘ | Update succeeded | Aug 30, 2015 20:00 |
| ⚠ | Policy non-compliance: Malware Protection | Aug 30, 2015 17:59 |
| ❗ | Real time protection disabled | Aug 30, 2015 17:59 |

## *Malware alerts*

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:



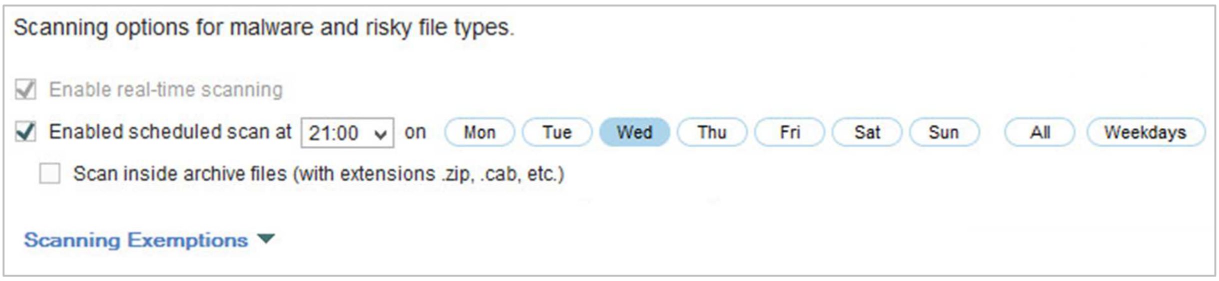
## *Program version*

We could not find a means of displaying the program version of the client software in the console.

## Managing the network

### *Scanning*

Scheduled Scans can be set in the console, by editing the policy applied to each user or group, as shown below.



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.)

An individual client device can be scanned from its properties page.

### *Updates*

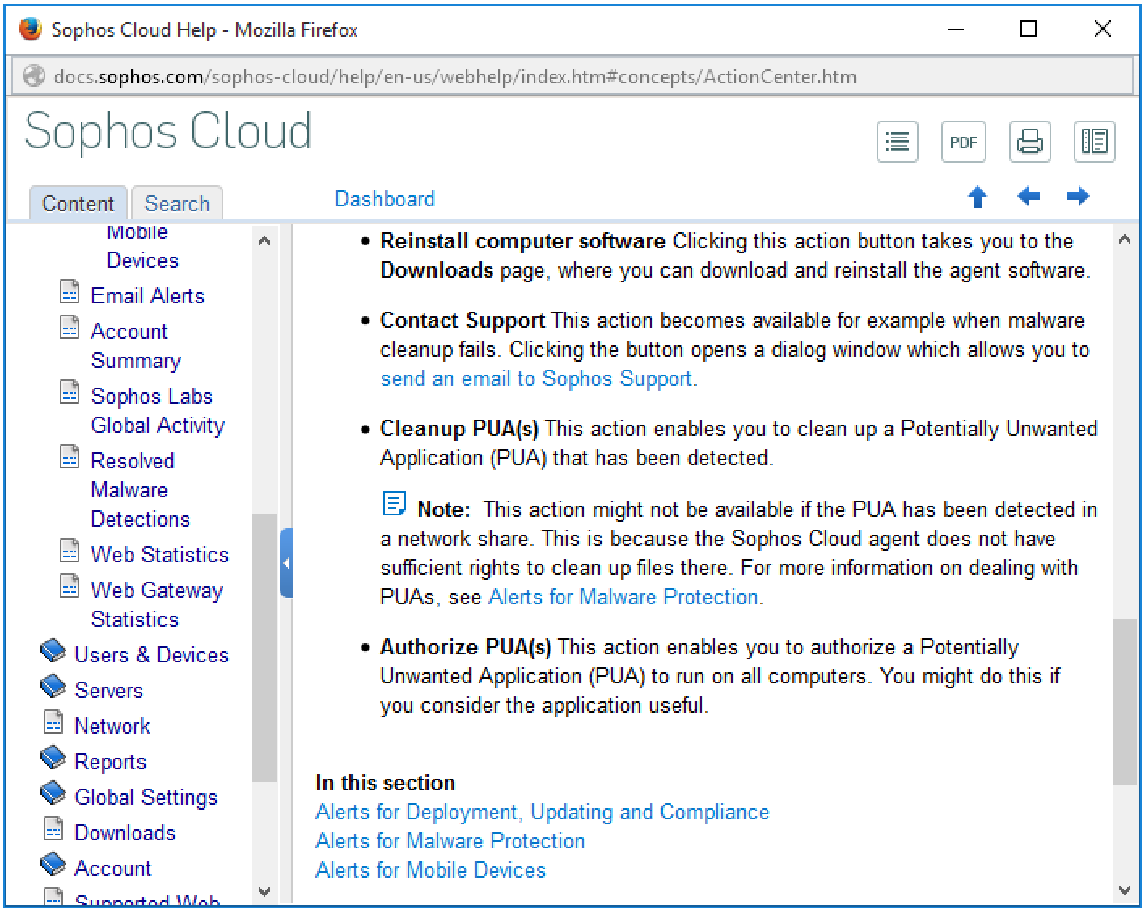
A manual update can be run on an individual computer by clicking the Users and Devices menu, Devices, and then the name of the computer concerned.

### *Removing devices from the console*

A device can be removed easily by selecting its checkbox on the *Devices* page, and clicking *Delete*.

### Integrated help feature

Clicking *Help* in the top right-hand corner of the console opens the product's web-based help feature. This is context-sensitive, i.e. it shows content relevant to the page of the console currently being viewed, which we find very convenient. A list of topics is displayed in a left-hand column, with simple, clear text instructions for the selected topic shown in the main panel:



- **Reinstall computer software** Clicking this action button takes you to the **Downloads** page, where you can download and reinstall the agent software.
- **Contact Support** This action becomes available for example when malware cleanup fails. Clicking the button opens a dialog window which allows you to send an email to Sophos Support.
- **Cleanup PUA(s)** This action enables you to clean up a Potentially Unwanted Application (PUA) that has been detected.

  **Note:** This action might not be available if the PUA has been detected in a network share. This is because the Sophos Cloud agent does not have sufficient rights to clean up files there. For more information on dealing with PUAs, see Alerts for Malware Protection.
- **Authorize PUA(s)** This action enables you to authorize a Potentially Unwanted Application (PUA) to run on all computers. You might do this if you consider the application useful.

**In this section**

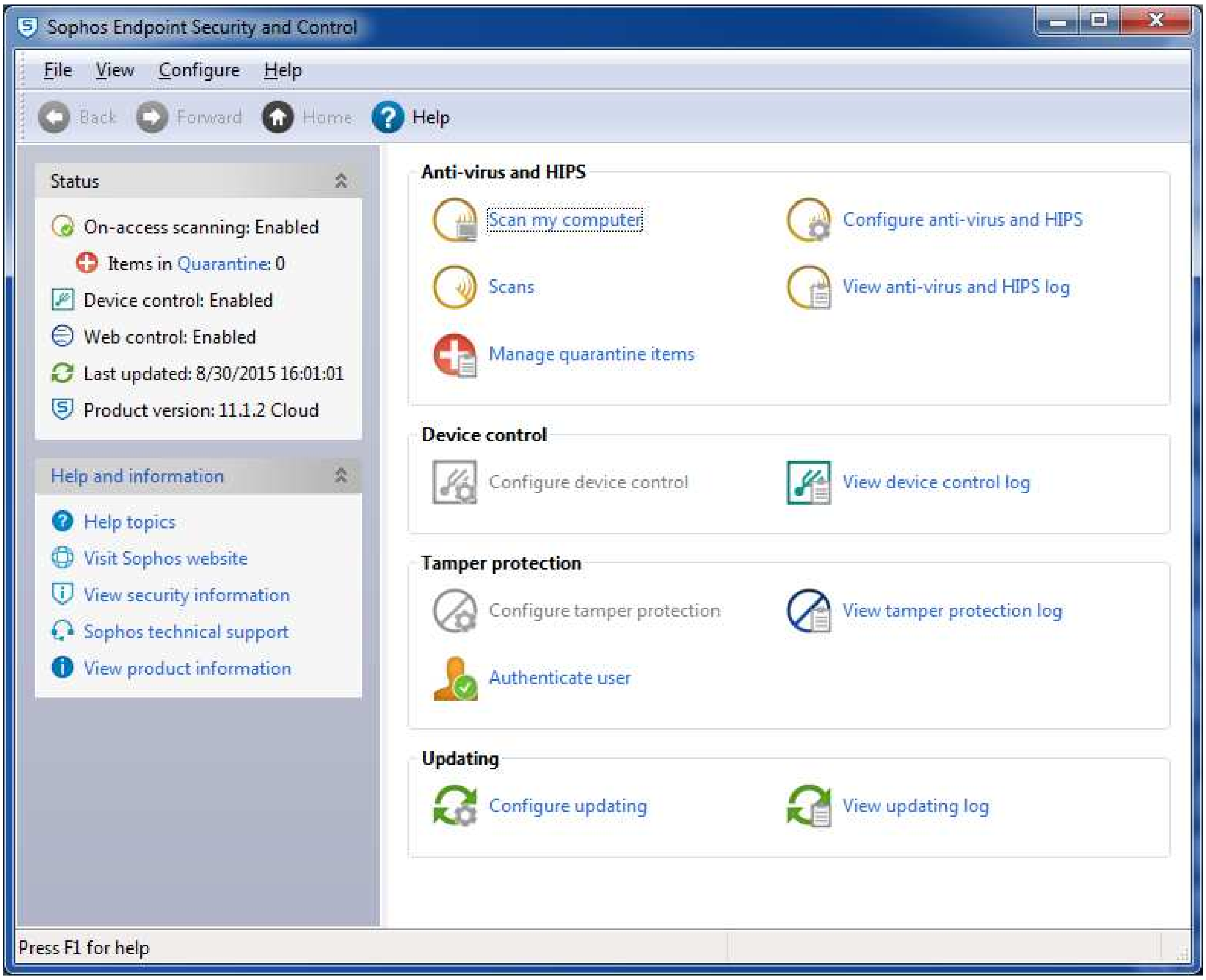
Alerts for Deployment, Updating and Compliance
Alerts for Malware Protection
Alerts for Mobile Devices

Clicking the *PDF* button in the top right-hand corner allows the admin to download the same content as a manual in .PDF format.

### Comment

Overall, we found Sophos' management console clear and easy to navigate, with important information and tasks easy to access. The help features are good. We were impressed with the automatic re-activation/reinstallation of disabled or uninstalled software, though we did wonder whether this might not be done more quickly, or an alert shown in the intervening period. We note that security policies apply to users rather than devices; Sophos inform us that a policy thus follows a user across multiple devices and platforms.

## Windows client protection software



Sophos Endpoint Security and Control

Status

On-access scanning: Enabled

Items in Quarantine: 0

Device control: Enabled

Web control: Enabled

Last updated: 8/30/2015 16:01:01

Product version: 11.1.2 Cloud

Press F1 for help

### Installation

To install the windows client software, the admin runs the .EXE installer file downloaded from the console. The only decision to make is whether to remove existing third-party security software; the process completes with a few clicks.

### Main program window

The main program window shows the status of protection components in the top left-hand corner. Users can run full and custom scans.

### Windows Security Center/Windows Defender

Sophos ESC registers as antivirus and antispyware in Windows Security Center. Under Windows 7, Windows Defender is not disabled.

### System Tray icon

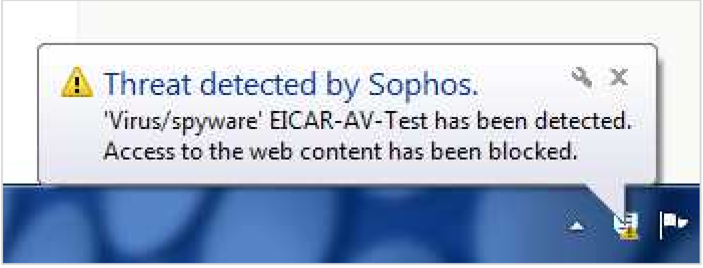
A System Tray icon is installed; right-clicking it allows the user to open the program or run an update.

### Unauthorised access

When logged on with a standard user account, the configuration options which would allow the user to deactivate protection in Sophos Cloud are deactivated. The *Tamper Protection* feature of the suite additionally allows the admin to password-protect the settings for all users, regardless of their Windows local/domain account type.

### Malware alerts

The following alert is shown when malware is discovered:



Threat detected by Sophos.
'Virus/spyware' EICAR-AV-Test has been detected.
Access to the web content has been blocked.

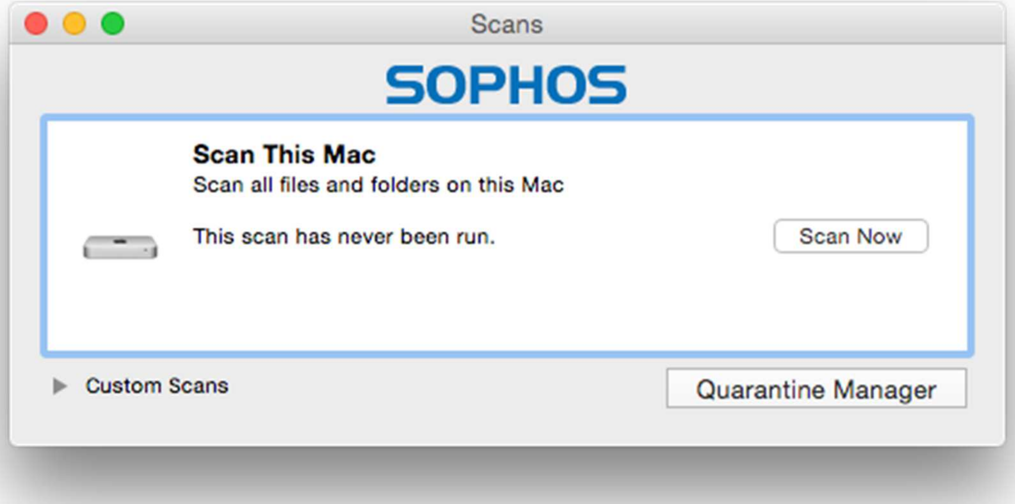
## Windows server protection software

Whilst the server protection software has a separate installer file, in terms of installation and user interface it can be regarded as being identical to the client. Sophos tell us that the management interface is different, and that there is a different configuration in the server software, to allow for e.g. Exchange or SQL running on the server.

### Comment

The Windows protection software allows users to perform essential tasks, i.e. run updates and scans, but not disable protection, which we find ideal. Although it is a very minor point, we wonder whether the graphical user interface, very similar to Windows XP's Explorer, might not give users the wrong message about continuing to use the now-unsupported 2001 operating system.

## Mac client protection software



Scan This Mac

Scan all files and folders on this Mac

This scan has never been run.

### Installation

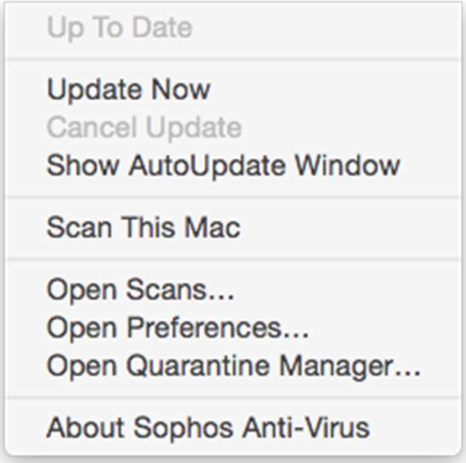
A .ZIP file is downloaded from the console. The admin runs the *Sophos Installer* within this; the installation then completes with a couple of clicks. There are no choices to be made.

### Main program window

Sophos Cloud Endpoint for Mac does not have a main program window as such. Scans can be run from the Scans dialog box, shown above; updates can be run from the System Tray menu, shown below. There is a sort of minimalist status display, in that when protection is disabled, the Sophos icon in the System Tray will be greyed out.

### System Tray icon

This displays the following menu:

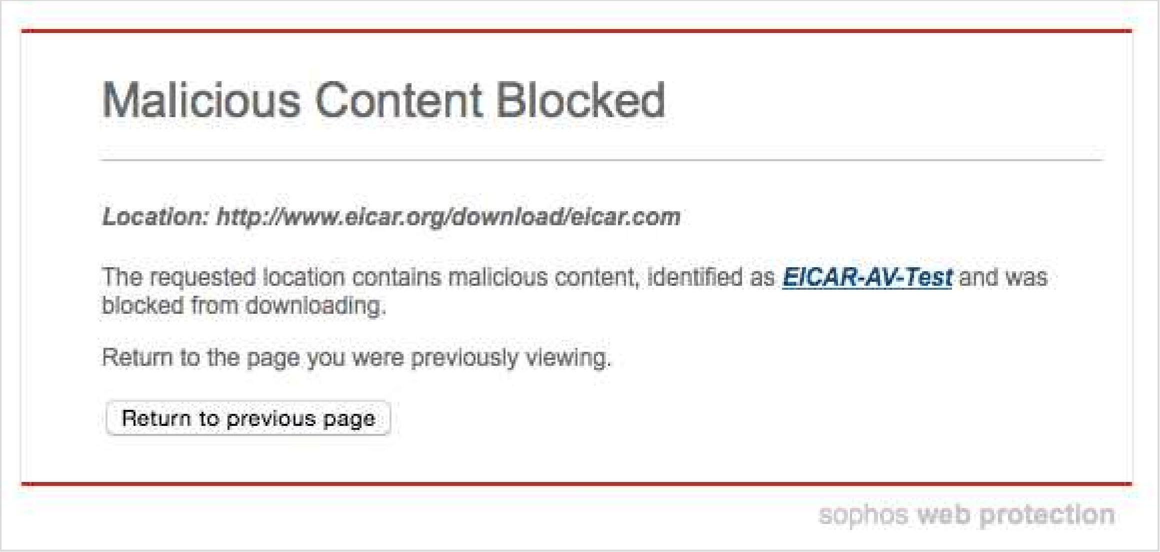


### Unauthorised access

Protection cannot be disabled without entering administrator credentials. *Tamper Protection* can also be enabled, as for the Windows software.

## Malware alerts

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



Malicious Content Blocked

*Location: http://www.eicar.org/download/eicar.com*

The requested location contains malicious content, identified as ***EICAR-AV-Test*** and was blocked from downloading.

Return to the page you were previously viewing.

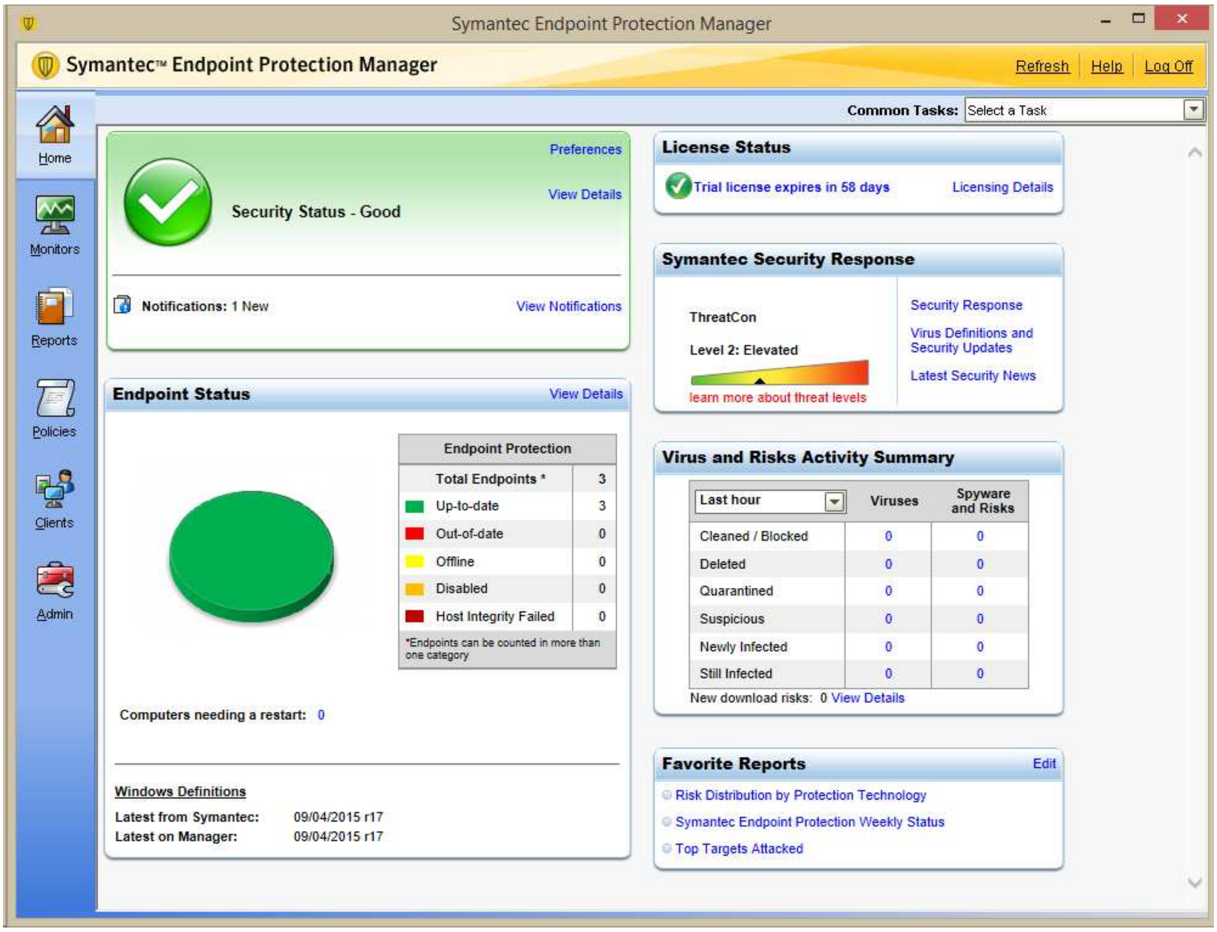
## Comment

Although the somewhat minimalist interface of Sophos Cloud Endpoint for Mac may seem unusual to some admins, it allows users to run updates and scans, but not to disable the protection. From a practical point of view, we would regard it as good.

## Summary

We feel that Sophos Cloud could be used by a non-expert administrator quite comfortably. The console is simple and clearly laid out, making it easy to find essential information and tasks, and the help features are good. Client software may be unusual in its design but is very practical. We also felt that the automatic reactivation/reinstallation of disabled/removed client software was very good, albeit somewhat slow to kick in.

# Symantec Endpoint Protection



Symantec Endpoint Protection Manager
Symantec™ Endpoint Protection Manager
Refresh
Help
Log Off
Home
Monitors
Reports
Policies
Clients
Admin
Common Tasks: Select a Task

Preferences
View Details
Security Status - Good
Notifications: 1 New View Notifications

**Endpoint Status** View Details

| Endpoint Protection | |
|---|---|
| Total Endpoints * | 3 |
| 🟩 Up-to-date | 3 |
| 🟥 Out-of-date | 0 |
| 🟨 Offline | 0 |
| 🟧 Disabled | 0 |
| 🟥 Host Integrity Failed | 0 |

*Endpoints can be counted in more than one category

Computers needing a restart: 0

Windows Definitions
Latest from Symantec: 09/04/2015 r17
Latest on Manager: 09/04/2015 r17

**License Status**
Trial license expires in 58 days Licensing Details

**Symantec Security Response**
ThreatCon
Level 2: Elevated
learn more about threat levels
Security Response
Virus Definitions and Security Updates
Latest Security News

**Virus and Risks Activity Summary**

| Last hour | Viruses | Spyware and Risks |
|---|---|---|
| Cleaned / Blocked | 0 | 0 |
| Deleted | 0 | 0 |
| Quarantined | 0 | 0 |
| Suspicious | 0 | 0 |
| Newly Infected | 0 | 0 |
| Still Infected | 0 | 0 |

New download risks: 0 View Details

**Favorite Reports** Edit
- Risk Distribution by Protection Technology
- Symantec Endpoint Protection Weekly Status
- Top Targets Attacked

## Introduction

Symantec produces a wide variety of security software for large and small businesses. For this review, we tested Endpoint Protection, which uses a Windows-based on-premise console to manage client protection software.

## Software versions reviewed

Symantec Endpoint Protection Manager 12.1.6306.6100 (12.1.6 MP1)
Symantec Endpoint Protection Client for Windows 12.1.6306.6100 (12.1.6 MP1)
Symantec Endpoint Protection Client for Mac 12.1.6168.6000 (12.1.6)

## Supported operating systems

Windows clients: Windows XP, XP Embedded*, Vista*, 7, 8, 8.1, 10*
(* = Endpoint Protection client only)
Windows servers: Windows Server 2003/R2, 2008/R2, 2012/R2; Windows Small Business Server 2003, 2008, 2011; Windows Essential Business Server 2008
Mac clients: Mac OS X 10.8, 10.9, 10.10

## Documentation

### Manuals

Symantec provides an extensive range of manuals for Endpoint Protection. Of these, the Installation and Administration Guide is the most comprehensive at 844 pages. It is very detailed, but easy to navigate via a clickable contents page and bookmarks. The instructions are very clearly written, although there are unfortunately no screenshots. There is also a 9-page Quick Start Guide available, covering the essentials of installing the console and deploying client software. This is very simply formatted and does not have a contents page, but explains the basics clearly with a number of screenshots.

### Knowledge base

There is an extensive knowledge base which can be searched for relevant articles.

### Comment

We suggest that the Quick Start Guide would be a good starting point for an inexperienced system administrator, while the Administration Guide should be ideal for experienced IT professionals, especially if managing larger networks.

## Management Console

### Installation and configuration

The console is installed on the Windows server by downloading and running an .EXE installer file. The setup wizard is extremely simple and only requires the admin to accept the licence agreement and choose the location of the installation folder.

### Layout

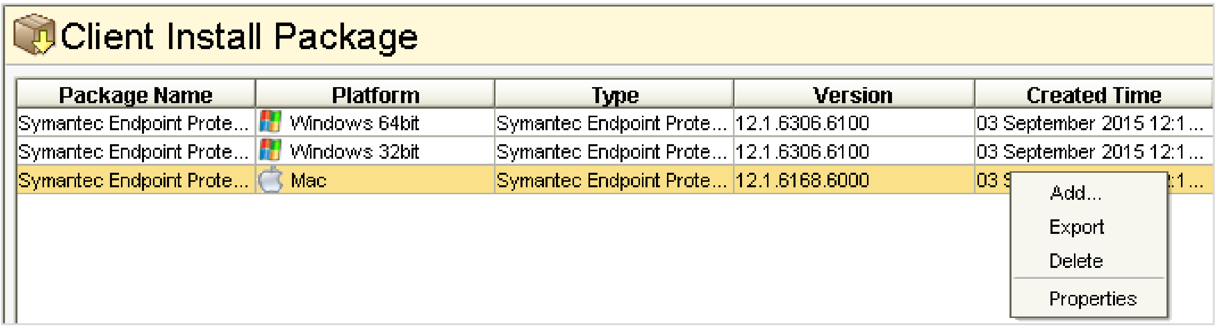
The main console window has a narrow menu column on the left-hand side, with the entries *Home, Monitors, Reports, Policies, Clients* and *Admin*. The *Home* page provides various panels showing the status of different items, including overall security status, status of endpoint clients, and licences.

### Preparing devices for deployment

We did not need to make any special configuration of the clients in order to use the local installation method.

### Deploying the endpoint protection software

There are three principal methods of deploying the client software: creating an installation package to use for local installation, emailing users with a link to the installer file, or using a remote push installation from the server. We used the local installation method in our test.
To do this, we exported installation packages for both Mac and Windows clients by going to the *Admin* page, *Install packages* tab. The admin then only needs to right-click the appropriate installer package and then click *Export*:



Client Install Package

| Package Name | Platform | Type | Version | Created Time |
|---|---|---|---|---|
| Symantec Endpoint Prote... | Windows 64bit | Symantec Endpoint Prote... | 12.1.6306.6100 | 03 September 2015 12:1... |
| Symantec Endpoint Prote... | Windows 32bit | Symantec Endpoint Prote... | 12.1.6306.6100 | 03 September 2015 12:1... |
| Symantec Endpoint Prote... | Mac | Symantec Endpoint Prote... | 12.1.6168.6000 | 03 S... :1... |

An .EXE file for Windows, or a .ZIP file for Mac, can then be saved to e.g. a network share or flash drive, from where it can be run on the client.

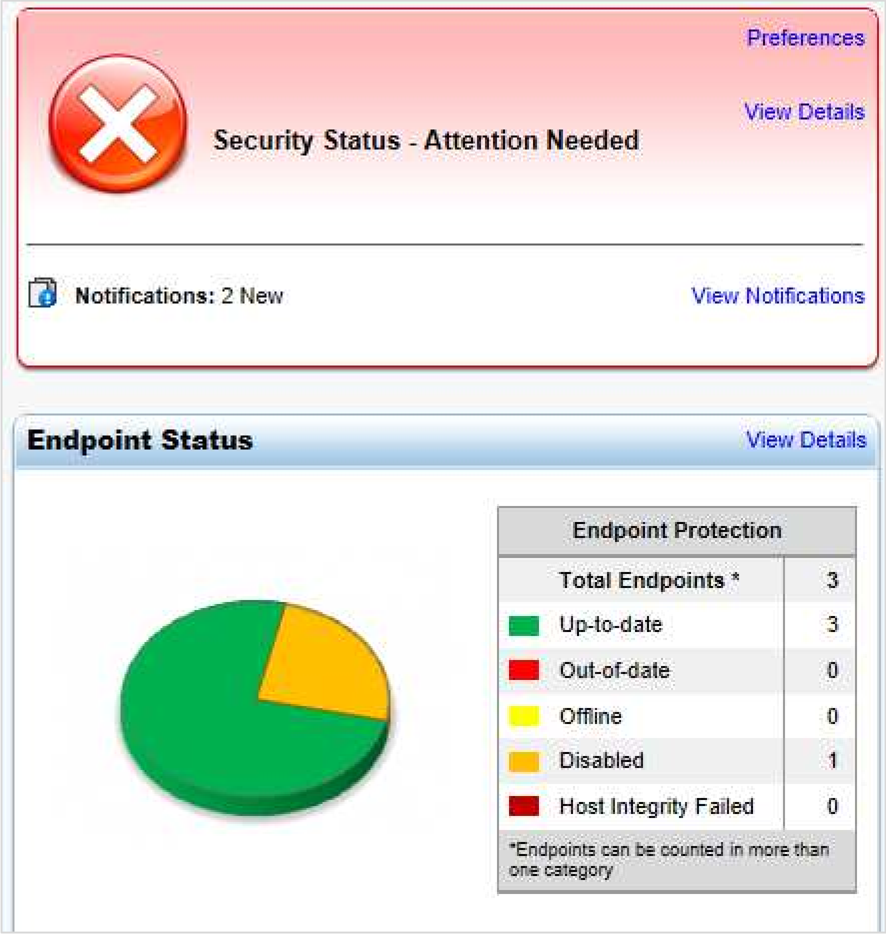
## Monitoring the network

### *Status*

This is shown in the *Security Status* and *Endpoint Status* panels on the Home page.

### *Warnings*

If protection is disabled on a client, the two status panels change as shown below:



Preferences

View Details

Security Status - Attention Needed

Notifications: 2 New

View Notifications

Endpoint Status

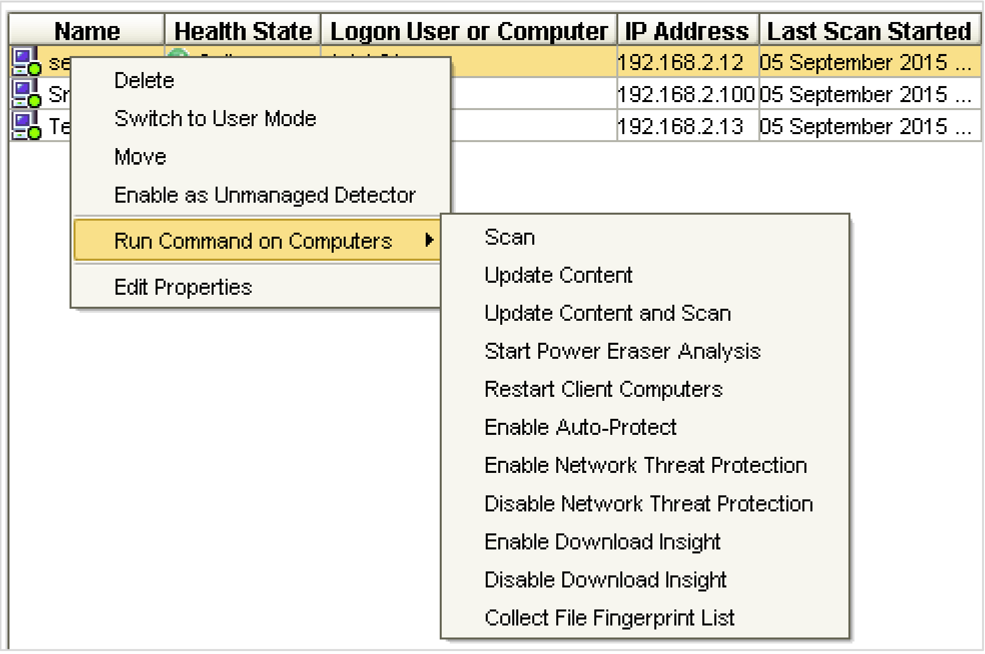
View Details

| Endpoint Protection | | |
|---|---|---|
| | Total Endpoints * | 3 |
| 🟩 | Up-to-date | 3 |
| 🟥 | Out-of-date | 0 |
| 🟨 | Offline | 0 |
| 🟧 | Disabled | 1 |
| 🟥 | Host Integrity Failed | 0 |

*Endpoints can be counted in more than one category

### *Rectifying problems*

Clicking *View Details* in the Security Status panel shows a list of protection components, and which of them is disabled on which client. The admin then goes to the *Clients* page and right-clicks the client PC(s) in question, and selects the appropriate command (e.g. *Enable Auto-Protect*):



| Name | Health State | Logon User or Computer | IP Address | Last Scan Started |
|---|---|---|---|---|
| se | | | 192.168.2.12 | 05 September 2015 ... |
| Sr | | | 192.168.2.100 | 05 September 2015 ... |
| Te | | | 192.168.2.13 | 05 September 2015 ... |

### *Malware alerts*

We found that when we downloaded the EICAR test file or AMTSO PUA test file – both of which were immediately detected and dealt with by the endpoint protection software – nothing was shown in the *Virus and Risks Activity Summary* panel on the home page of the console. Symantec tell us that with default settings, EICAR events are deleted from risk logs. However, creating a report on the *Reports* page did show all instances of such detections, however.

### *Program version*

This can be displayed for any individual client by double-clicking the device's entry in the *Clients* tab of the *Clients* page. Symantec tell us that it can be shown for all clients by going to *Monitors* > *Client Status* > *View log, or Reports* > *Computer Status, SEP Product Versions* > *Create report*.

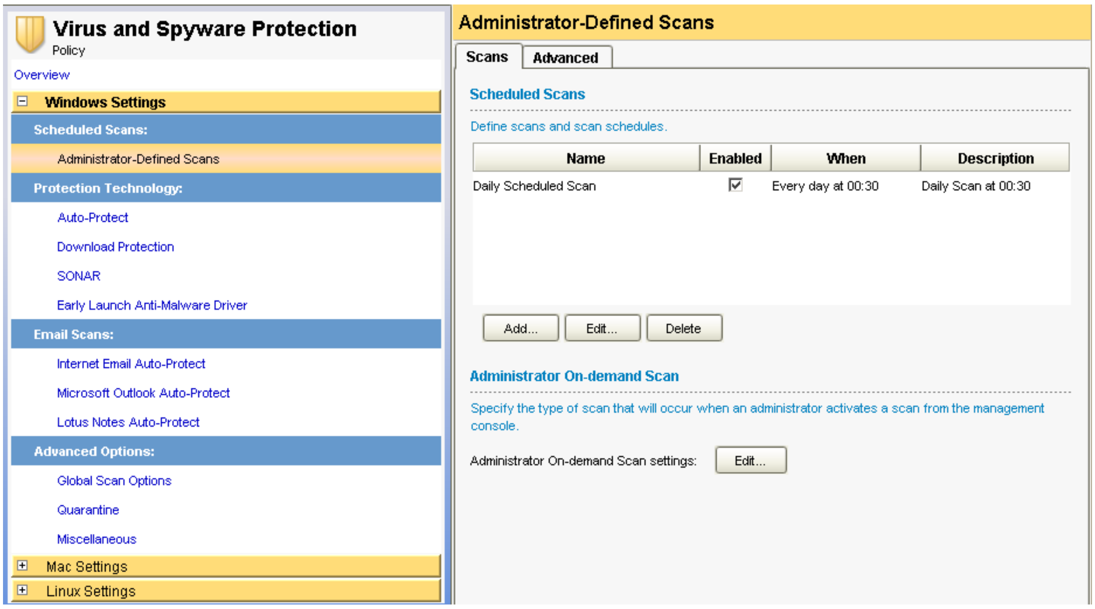
## Managing the network

### *Scanning*

Scans can be run from *Clients/Clients* by selecting the relevant device or devices (standard Windows selection techniques such as Ctrl + A, Ctrl + click can be used to make multiple selections), right-clicking, and clicking *Scan*. A choice of quick, full or custom scans is provided.

### *Scheduling Scans*

Scheduled scans can be configured by going to the *Policies* page of the console and editing an existing policy or creating a new one. By default, a scheduled scan runs at 00:30 every day:



Define scans and scan schedules.

| Name | Enabled | When | Description |
|---|---|---|---|
| Daily Scheduled Scan | ☑ | Every day at 00:30 | Daily Scan at 00:30 |

Specify the type of scan that will occur when an administrator activates a scan from the management console.

Administrator On-demand Scan settings:

## Updates

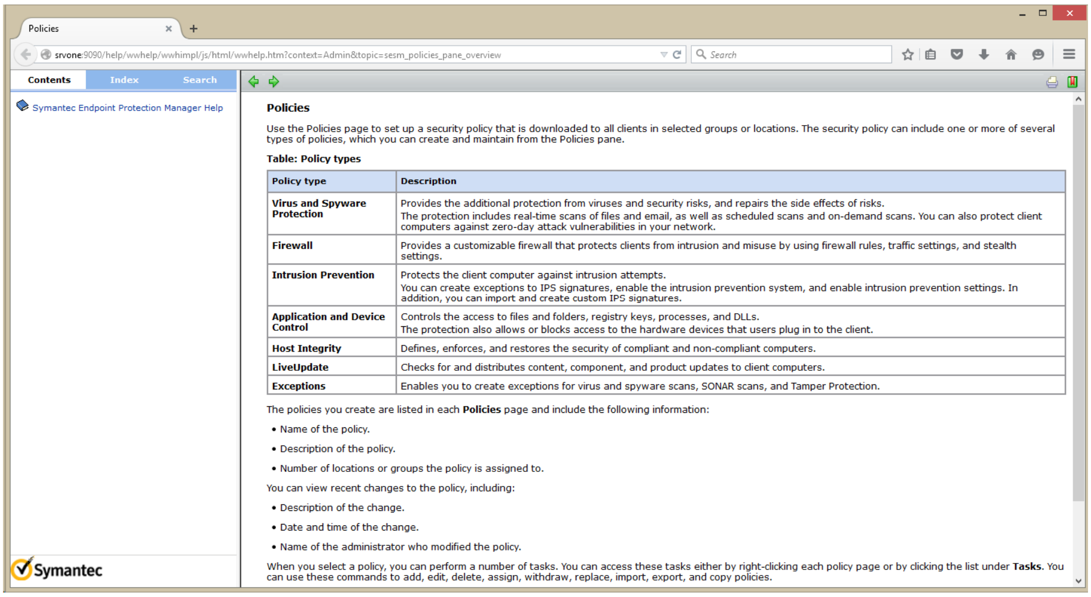
Running an update is identical to the scanning procedure described above, except that the admin clicks *Update Content*.

## Removing devices from the console

A device can be removed very simply by right-clicking its entry under *Clients/Clients* and clicking *Delete*.

## Integrated help feature

Clicking the *Help* link in the top right-hand corner of the console opens the local web-based help feature. This is context sensitive, i.e. it opens the help page relevant to the current feature being used on the console.


Policies
srvone:9090/help/wwhelp/wwhimpl/js/html/wwhelp.htm?context=Admin&topic=sesm_policies_pane_overview
Search
Contents
Index
Search
Symantec Endpoint Protection Manager Help
Symantec

**Policies**

Use the Policies page to set up a security policy that is downloaded to all clients in selected groups or locations. The security policy can include one or more of several types of policies, which you can create and maintain from the Policies pane.

**Table: Policy types**

| Policy type | Description |
|---|---|
| **Virus and Spyware Protection** | Provides the additional protection from viruses and security risks, and repairs the side effects of risks.<br>The protection includes real-time scans of files and email, as well as scheduled scans and on-demand scans. You can also protect client computers against zero-day attack vulnerabilities in your network. |
| **Firewall** | Provides a customizable firewall that protects clients from intrusion and misuse by using firewall rules, traffic settings, and stealth settings. |
| **Intrusion Prevention** | Protects the client computer against intrusion attempts.<br>You can create exceptions to IPS signatures, enable the intrusion prevention system, and enable intrusion prevention settings. In addition, you can import and create custom IPS signatures. |
| **Application and Device Control** | Controls the access to files and folders, registry keys, processes, and DLLs.<br>The protection also allows or blocks access to the hardware devices that users plug in to the client. |
| **Host Integrity** | Defines, enforces, and restores the security of compliant and non-compliant computers. |
| **LiveUpdate** | Checks for and distributes content, component, and product updates to client computers. |
| **Exceptions** | Enables you to create exceptions for virus and spyware scans, SONAR scans, and Tamper Protection. |

The policies you create are listed in each **Policies** page and include the following information:

- Name of the policy.
- Description of the policy.
- Number of locations or groups the policy is assigned to.

You can view recent changes to the policy, including:

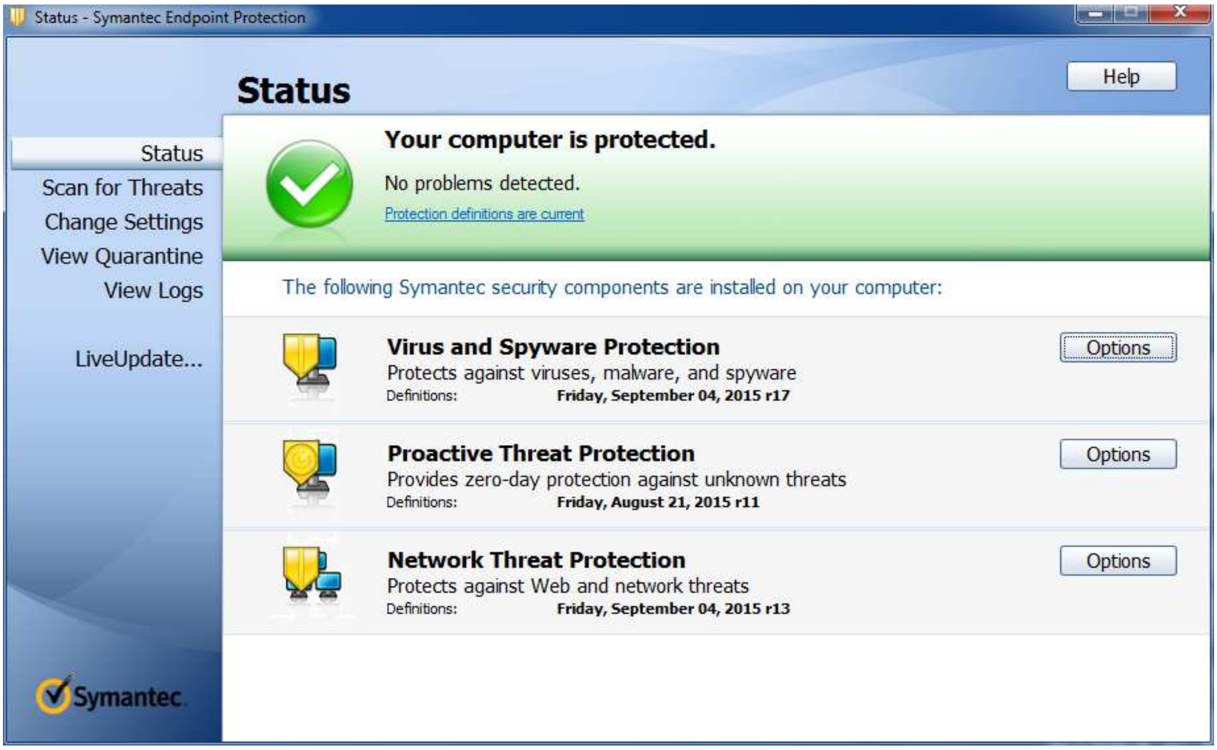
- Description of the change.
- Date and time of the change.
- Name of the administrator who modified the policy.

When you select a policy, you can perform a number of tasks. You can access these tasks either by right-clicking each policy page or by clicking the list under **Tasks**. You can use these commands to add, edit, delete, assign, withdraw, replace, import, export, and copy policies.

## Comment

Although the console is obviously very powerful and capable of handling large networks and a multitude of configuration options, we were still able to find essential monitoring and management functions without any difficulty.

### Windows client protection software



Status - Symantec Endpoint Protection

Status

Your computer is protected.

No problems detected.

Protection definitions are current

The following Symantec security components are installed on your computer:

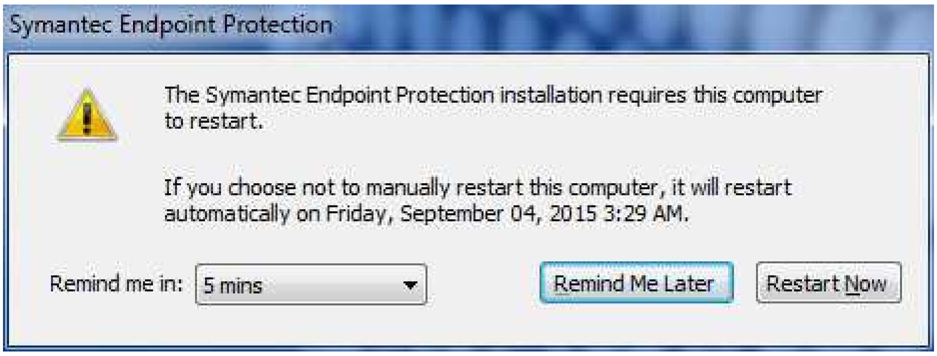
**Virus and Spyware Protection**
Protects against viruses, malware, and spyware
Definitions: Friday, September 04, 2015 r17

**Proactive Threat Protection**
Provides zero-day protection against unknown threats
Definitions: Friday, August 21, 2015 r11

**Network Threat Protection**
Protects against Web and network threats
Definitions: Friday, September 04, 2015 r13

### Installation

This is a very simple process. Having started the installer, the admin only needs to restart the computer at the end:



Symantec Endpoint Protection

The Symantec Endpoint Protection installation requires this computer to restart.

If you choose not to manually restart this computer, it will restart automatically on Friday, September 04, 2015 3:29 AM.

Remind me in: 5 mins

### Main program window

This provides similar functionality to a consumer antivirus program. There is a status display, which shows a warning and a "Fix All" button if protection is disabled. All users can run updates and scans and access the help; administrators can additionally change the settings.

### Windows Security Center/Windows Defender

The Symantec Endpoint Protection client registers as firewall, antivirus and antispyware. Under Windows 7, Windows Defender is disabled.

### System Tray icon

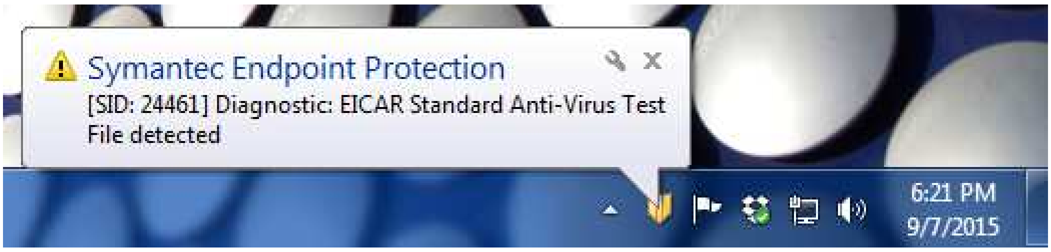
A System Tray icon is installed; right-clicking it allows the admin to open the program, update policy, or disable protection.

### Unauthorised access

When a user logs on with a standard Windows user account, the options for disabling protection are greyed out (deactivated).

### Malware alerts

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



Symantec Endpoint Protection
[SID: 24461] Diagnostic: EICAR Standard Anti-Virus Test File detected

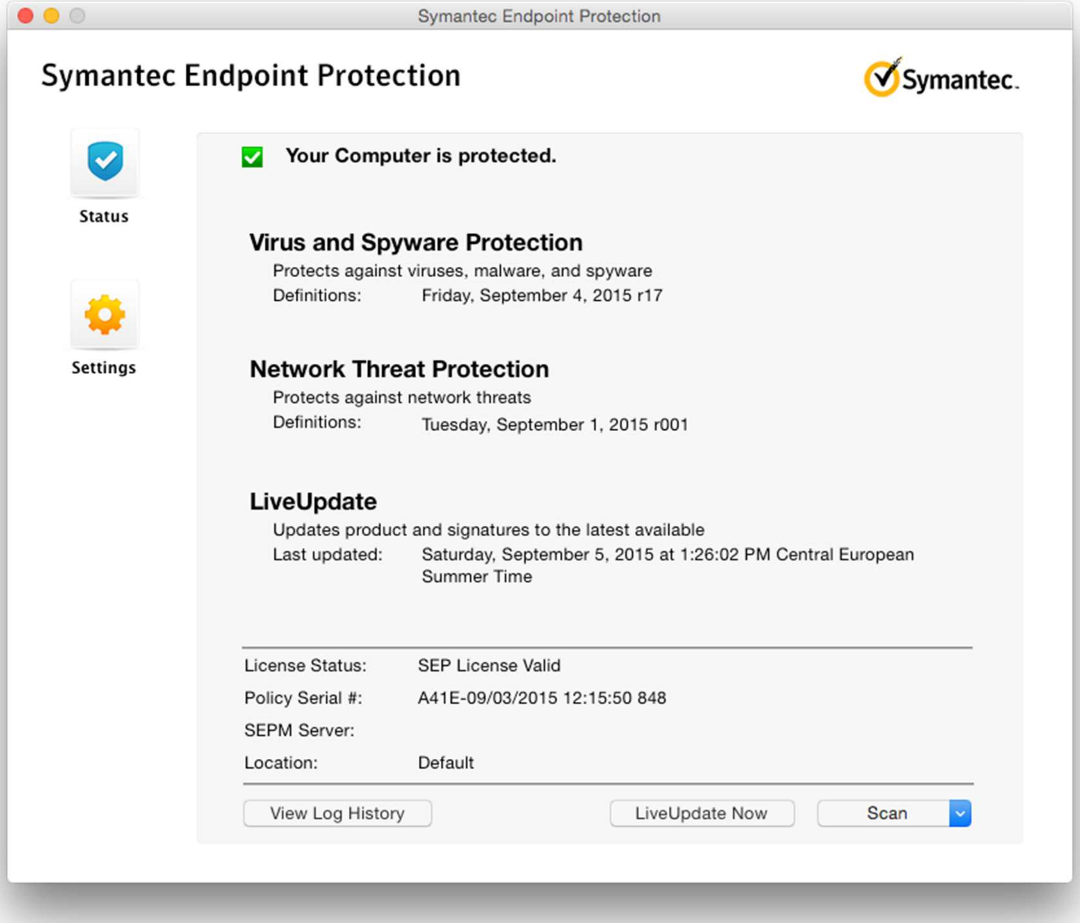
## Windows server protection software

In terms of installation and user interface, this can be regarded as identical to the Windows client software.

### Comment

We feel the client software should be very familiar to anyone who has used a typical Windows consumer antivirus product, and provides appropriate functionality for administrators and standard users respectively.

## Mac client protection software


Symantec Endpoint Protection

Symantec Endpoint Protection

☑ Your Computer is protected.

Virus and Spyware Protection
Protects against viruses, malware, and spyware
Definitions: Friday, September 4, 2015 r17

Network Threat Protection
Protects against network threats
Definitions: Tuesday, September 1, 2015 r001

LiveUpdate
Updates product and signatures to the latest available
Last updated: Saturday, September 5, 2015 at 1:26:02 PM Central European Summer Time

License Status: SEP License Valid
Policy Serial #: A41E-09/03/2015 12:15:50 848
SEPM Server:
Location: Default

### Installation

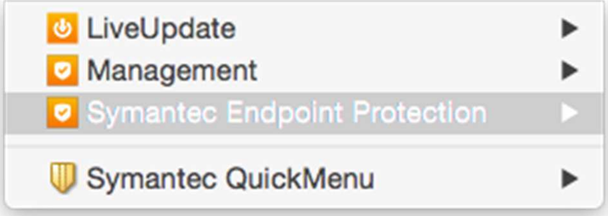
This is a very simple process. The administrator simply has to run the installer file and restart the computer when it has finished.

### Main program window

This provides a status display and access to essential functions such as scans, updates and help, in a familiar interface. If a protection component is disabled, the text and symbol of the status display change accordingly, and a *Fix* button appears to reactivate the protection.

### System Tray icon

The System Tray icon displays the following sub-menus:



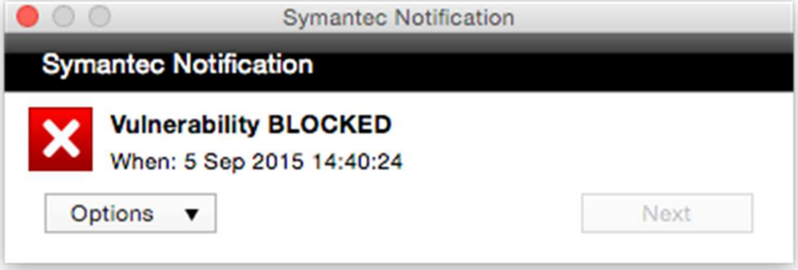
Amongst the available functions are opening the main window, running updates and opening the settings.

### Unauthorised access

A standard user cannot disable the protection unless administrator credentials are entered.

### Malware alerts

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



Symantec Notification

Symantec Notification

Vulnerability BLOCKED

When: 5 Sep 2015 14:40:24

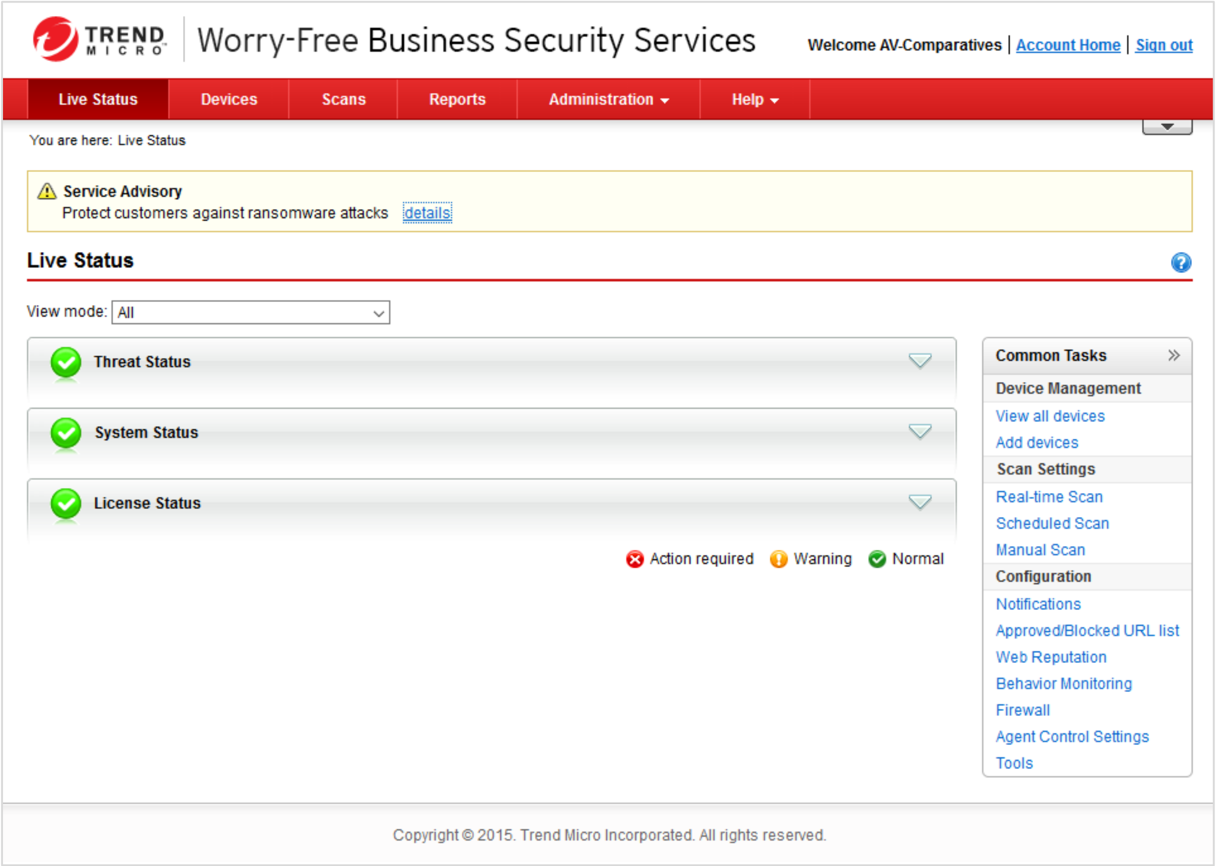
### Comment

Like its Windows counterpart, the Mac client software provides essential functionality in a familiar interface, whilst preventing non-administrators from disabling protection.

## Summary

Symantec Endpoint Protection includes a wide range of functionality and configuration options, and has the capacity to cope with very sizeable business networks. Nonetheless it could also be used by smaller businesses. We feel the console is easy to navigate, and we had no difficulty finding essential monitoring and management features. The endpoint protection software for Windows clients, the Windows server and Mac clients will be very familiar and easy to use for anyone familiar with standard consumer security programs. Documentation is very comprehensive.

# Trend Micro Worry-Free Business Security Services



You are here: Live Status

⚠ Service Advisory
Protect customers against ransomware attacks details

Live Status

View mode: All

✓ Threat Status

✓ System Status

✓ License Status

✕ Action required ! Warning ✓ Normal

Copyright © 2015. Trend Micro Incorporated. All rights reserved.

## Introduction

Trend Micro produce a range of enterprise solutions, suitable for larger companies, while Worry-Free Business Security Services is aimed at small businesses with up to 100 users. It uses a cloud-based console to manage protection software for Windows and Mac clients.

## Software versions reviewed

Trend Micro Worry-Free Business Security Services 5.7 SP1
Windows client and server protection software: 5.7.2544/19.1.2512
Mac client protection software: 2.0.1210

## Supported operating systems

Windows clients: XP, Vista, 7, 8, 8.1, 10
Windows servers: Windows Server 2003, 2003 R2, 2008, 2008 R2, 2012, 2012 R2; Small Business Server 2003, 2003 R2, 2008, 2011
Mac clients: OS X 10.6, 10.7, 10.8, 10.9, 10.10
Android/iOS: please see feature list.

## Documentation

We were not able to find a manual or knowledge base articles that were relevant to the product being tested. We recommend users to look at the integrated help feature described below.

## Management Console

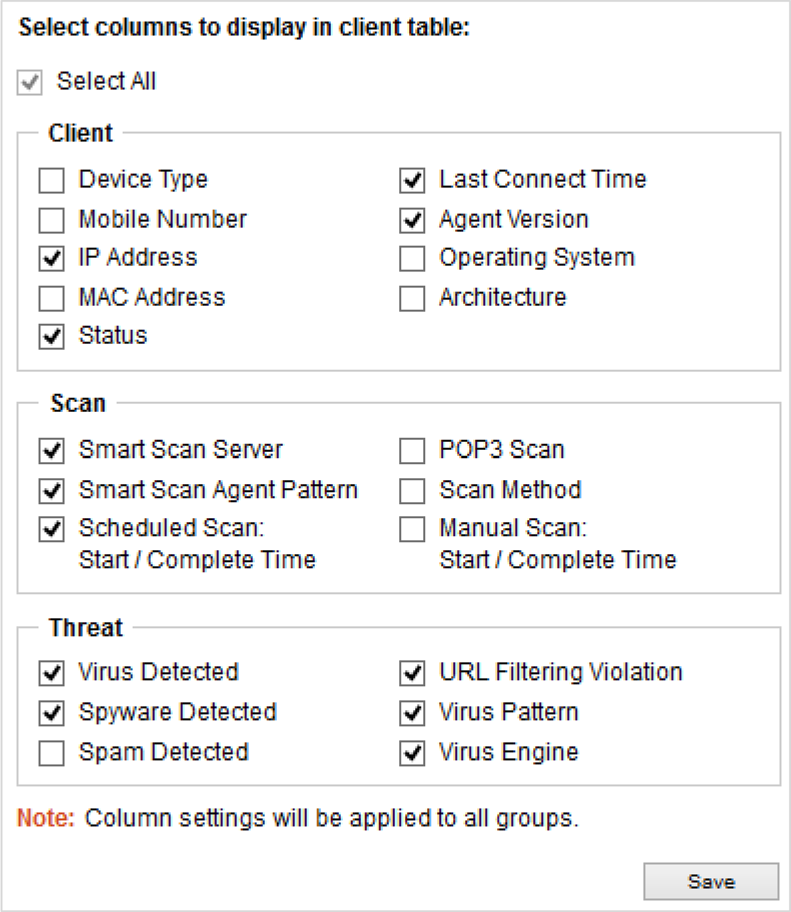
### Installation and configuration

No installation or configuration of the console is necessary, as it is cloud-based. The administrator simply logs in with a web browser.

### Layout

By default, the console opens on the *Live Status* tab, shown in the main screenshot above. This essentially shows whether all is well in the categories *Threat Status, System Status* and *License Status*, and shows a warning with details if not. There is a menu bar at the top of the console, with the tabs *Live Status, Devices, Scans, Reports, Administration* and *Help*. *Devices* shows a list of protected devices, and allows deployment of the protection software to new ones; *Scans* lets the administrator run and schedule scans; *Reports* can be used to generate customised reports of relevant events; *Administration* allows the admin to e.g. configure global settings and manage licences.

The *Devices* page can be customised by adding or removing columns:



**Select columns to display in client table:**

☑ Select All

**Client**

□ Device Type
□ Mobile Number
☑ IP Address
□ MAC Address
☑ Status
☑ Last Connect Time
☑ Agent Version
□ Operating System
□ Architecture

**Scan**

☑ Smart Scan Server
☑ Smart Scan Agent Pattern
☑ Scheduled Scan: Start / Complete Time
□ POP3 Scan
□ Scan Method
□ Manual Scan: Start / Complete Time

**Threat**

☑ Virus Detected
☑ Spyware Detected
□ Spam Detected
☑ URL Filtering Violation
☑ Virus Pattern
☑ Virus Engine

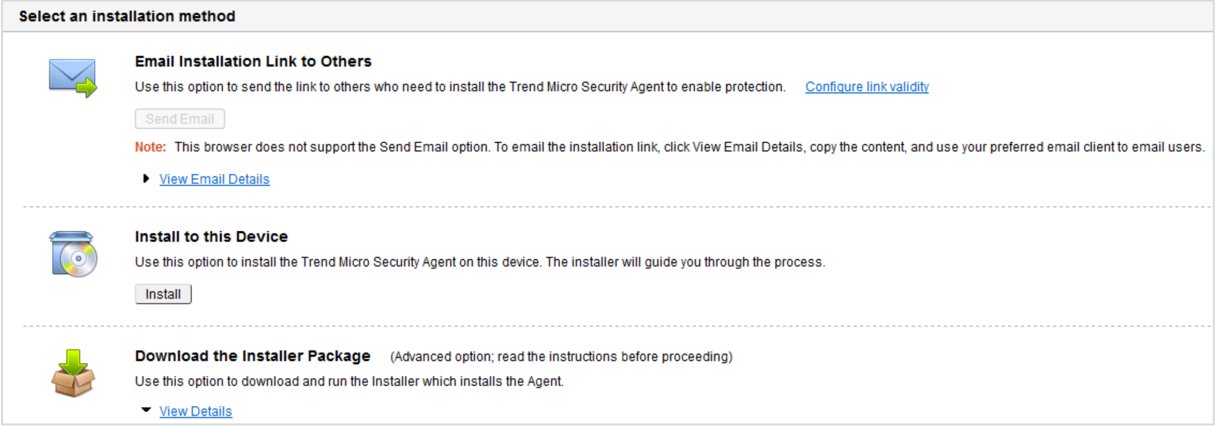
Note: Column settings will be applied to all groups.

### Preparing devices for deployment

We did not have to configure Windows or Mac clients before deploying the software by direct download.

### Deploying the endpoint protection software

Clicking the *Devices* tab, then *Add Devices*, opens the page of the same name. This provides 3 different deployment methods: sending an installation link to the user by email; local installation by direct download; creating an installer package which can be e.g. put on a network drive or flash drive to install multiple devices:



**Select an installation method**

**Email Installation Link to Others**

Use this option to send the link to others who need to install the Trend Micro Security Agent to enable protection. Configure link validity

Note: This browser does not support the Send Email option. To email the installation link, click View Email Details, copy the content, and use your preferred email client to email users.

**Install to this Device**

Use this option to install the Trend Micro Security Agent on this device. The installer will guide you through the process.

**Download the Installer Package** (Advanced option; read the instructions before proceeding)

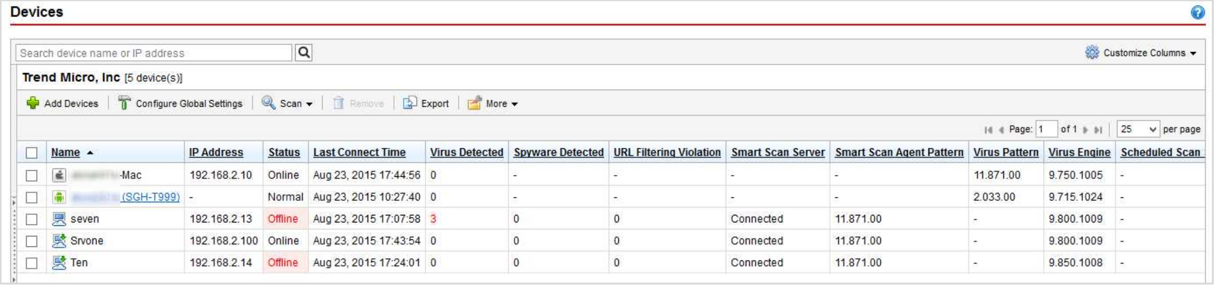
Use this option to download and run the Installer which installs the Agent.

In our test, we used the local installation by direct download from the console to install Windows and Mac clients.

## Monitoring the network

### *Status*

The default *Live Status* page of the console provides an overview of system status. For a more detailed view, the administrator can go to the *Devices* tab, which lists all protected devices and displays important information for each one:



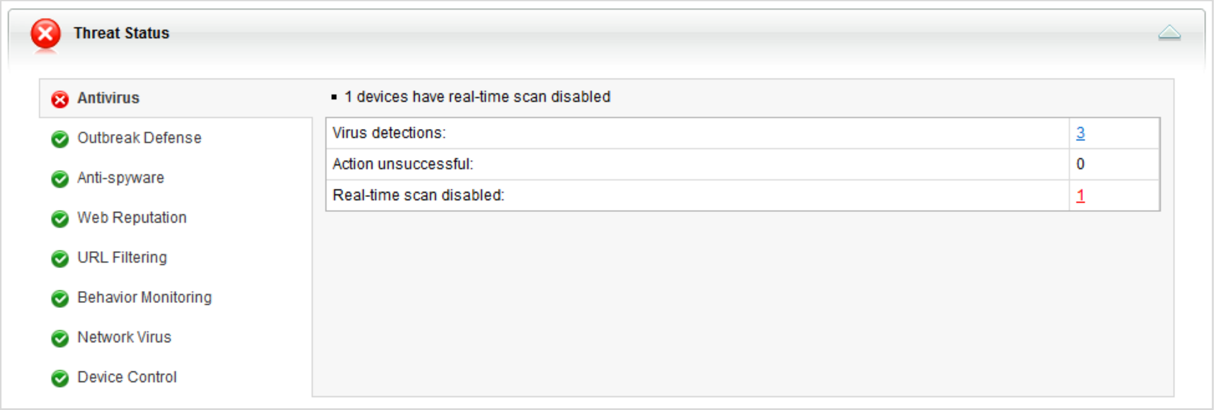
**Devices**

**Trend Micro, Inc** [5 device(s)]

| □ | Name ▲ | IP Address | Status | Last Connect Time | Virus Detected | Spyware Detected | URL Filtering Violation | Smart Scan Server | Smart Scan Agent Pattern | Virus Pattern | Virus Engine | Scheduled Scan |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | [redacted]-Mac | 192.168.2.10 | Online | Aug 23, 2015 17:44:56 | 0 | - | - | - | - | 11.871.00 | 9.750.1005 | - |
| □ | [redacted] (SGH-T999) | - | Normal | Aug 23, 2015 10:27:40 | 0 | - | - | - | - | 2.033.00 | 9.715.1024 | - |
| □ | seven | 192.168.2.13 | Offline | Aug 23, 2015 17:07:58 | 3 | 0 | 0 | Connected | 11.871.00 | - | 9.800.1009 | - |
| □ | Srvone | 192.168.2.100 | Online | Aug 23, 2015 17:43:54 | 0 | 0 | 0 | Connected | 11.871.00 | - | 9.800.1009 | - |
| □ | Ten | 192.168.2.14 | Offline | Aug 23, 2015 17:24:01 | 0 | 0 | 0 | Connected | 11.871.00 | - | 9.850.1008 | - |

### *Warnings*

The *Live Status* page displays a basic indication of any problems:



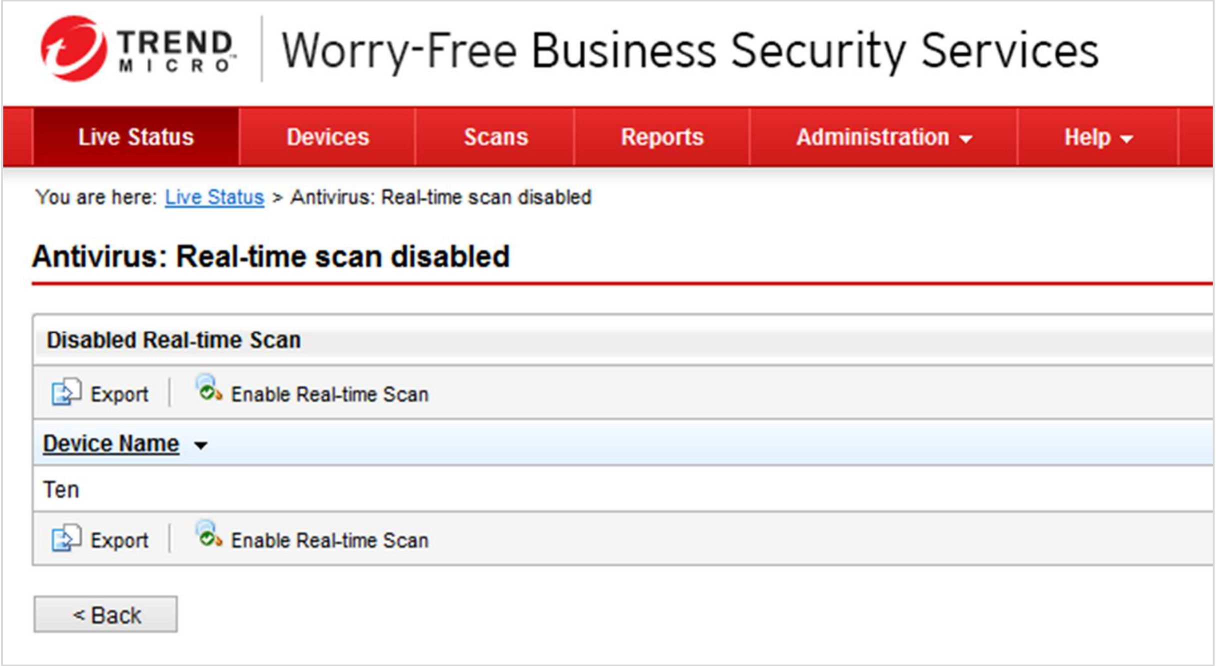
**Threat Status**

- 1 devices have real-time scan disabled

| | |
|---|---|
| Virus detections: | 3 |
| Action unsuccessful: | 0 |
| Real-time scan disabled: | 1 |

### *Rectifying problems*

Clicking on the number representing how many devices are affected opens a page from which the problem can be solved. For example, clicking the *1* at the end of the line *Real-time scan disabled* in the screenshot above opens the following page:



### *Malware alerts*

Malware detections are shown in the *Virus detected* column of the *Devices* page.

### *Program version*

This is shown on the *Devices* page, *Agent Version* column.

## Managing the network

### *Scanning*

Standard scans can be run by selecting the devices to be scanned in the *Devices* page using their checkboxes, then clicking *Scan Now* from the *Scan* menu on the toolbar. The same menu can be used to stop a running scan if desired.

### *Scheduling Scans*

The *Scans* tab, *Scheduled Scan* sub-tab allows the administrator to schedule daily, weekly or monthly scans. In each case, day and time of day can be specified. There are different settings for servers and endpoint devices.

### *Updates*

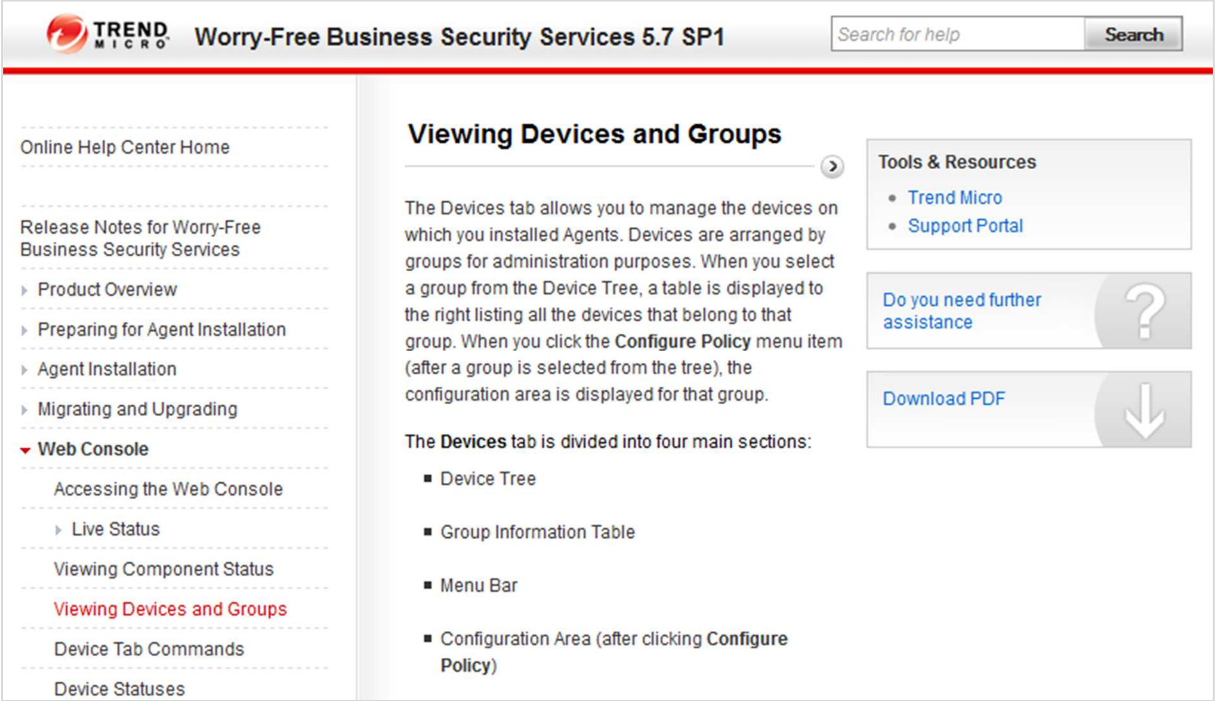
Devices can be updated from the *Devices* page, by selecting the relevant devices and clicking *Update Now* from the *More* menu.

### *Removing devices from the console*

This can be done very easily by clicking the relevant checkbox(es) on the *Devices* page, and then *Remove* on the toolbar.

## Integrated help feature

Clicking the *?* symbol in the top right-hand corner of the console opens the online help feature. This displays a list of features and tasks on the left-hand side, with simple text explanations/instructions shown in the main pane:



## Viewing Devices and Groups

The Devices tab allows you to manage the devices on which you installed Agents. Devices are arranged by groups for administration purposes. When you select a group from the Device Tree, a table is displayed to the right listing all the devices that belong to that group. When you click the **Configure Policy** menu item (after a group is selected from the tree), the configuration area is displayed for that group.

The **Devices** tab is divided into four main sections:

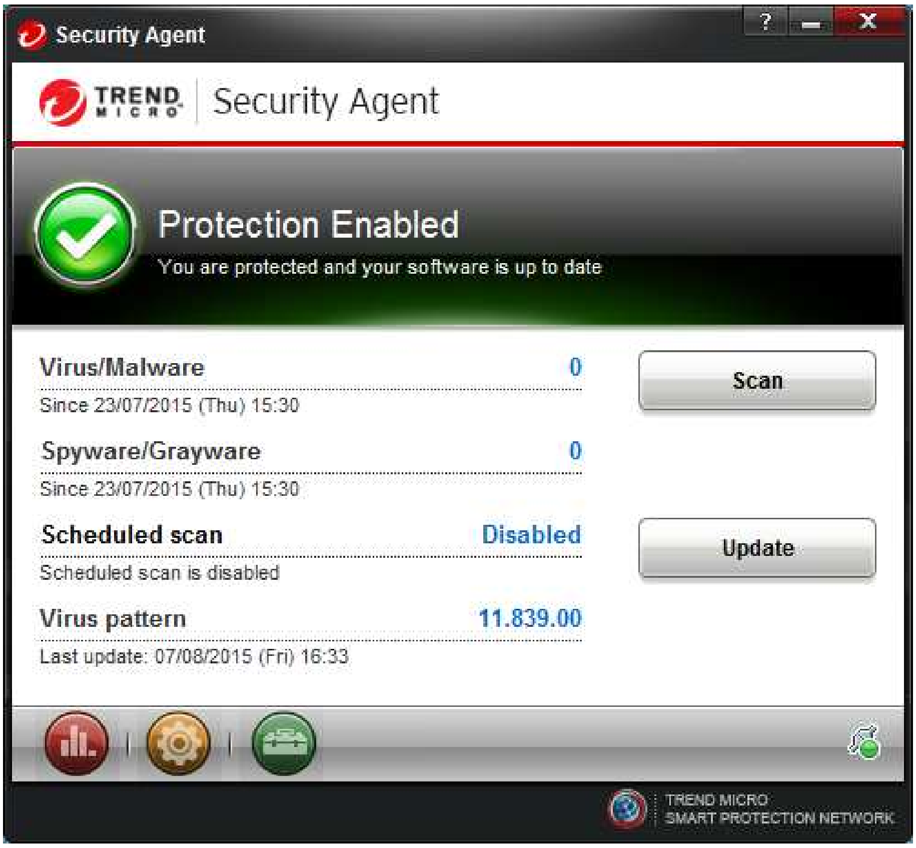
- Device Tree
- Group Information Table
- Menu Bar
- Configuration Area (after clicking **Configure Policy**)

## Comment

We found Trend Micro's console to be very largely intuitive to use, with almost all important information and tasks being easy to find on the *Devices* tab. We note that the administrator will need to check the *Live Status* tab as well, in order to check protection status and rectify any problems; however, this is shown by default every time the admin logs on.

We feel the integrated help feature, whilst comprehensive in its range of topics, provides quite spartan texts without any screenshots. We feel this is an area that could be improved, especially as we were unable to find a relevant manual or knowledge-base articles.

## Windows client protection software



Security Agent

TREND MICRO | Security Agent

Protection Enabled

You are protected and your software is up to date

Virus/Malware 0

Since 23/07/2015 (Thu) 15:30

Spyware/Grayware 0

Since 23/07/2015 (Thu) 15:30

Scheduled scan Disabled

Scheduled scan is disabled

Virus pattern 11.839.00

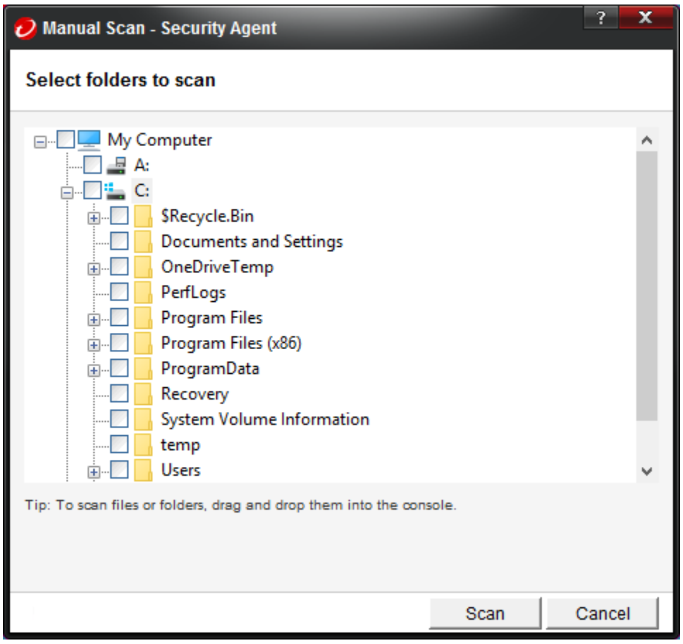
Last update: 07/08/2015 (Fri) 16:33

### Installation

This could hardly be simpler. Having downloaded and started the installer, the admin only needs to click *Next* and *Finish* to complete the wizard.

### Main program window

There is a prominent status display with text and an icon, along with buttons to run an update or scan. The latter allows the user to select the complete system, or individual folders, from a single dialog box:



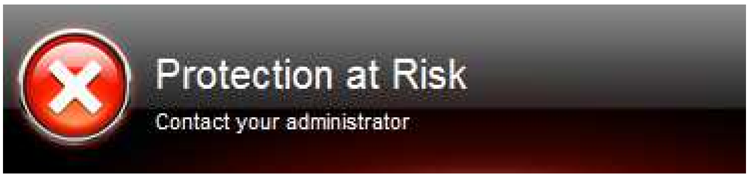
Manual Scan - Security Agent

Select folders to scan

- □ My Computer
  - □ A:
  - □ C:
    - □ $Recycle.Bin
    - □ Documents and Settings
    - □ OneDriveTemp
    - □ PerfLogs
    - □ Program Files
    - □ Program Files (x86)
    - □ ProgramData
    - □ Recovery
    - □ System Volume Information
    - □ temp
    - □ Users

Tip: To scan files or folders, drag and drop them into the console.

If real-time protection is disabled, the status display shows an alert, with the instruction to contact the administrator to rectify the problem:



Protection at Risk

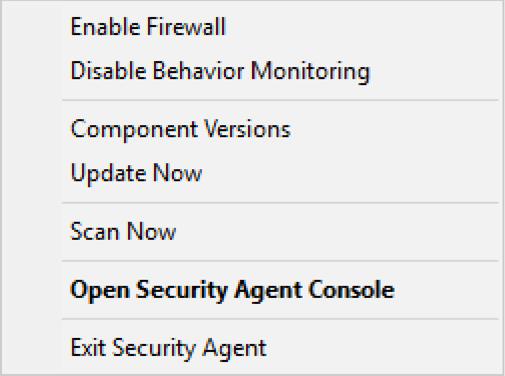
Contact your administrator

### Windows Security Center/Windows Defender

Trend Micro Security Agent registers as the antispyware and antivirus program. Under Windows 7, Windows Defender is not disabled.

### System Tray icon

This can be used to display the following menu:

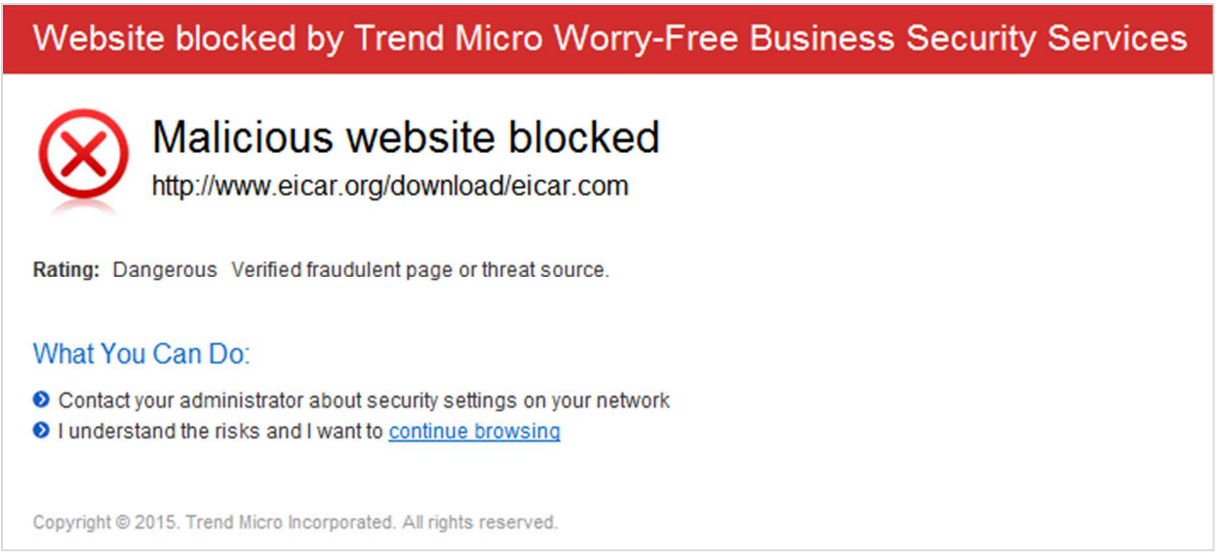


### Unauthorised access

Using a standard user account, we found it was possible to disable the Security Agent completely using the *Exit Security Agent* entry in the System Tray menu shown above. The device is then shown as offline in the *Devices* view of the console; a warning is not shown in the *Live Status* view. It is also possible to activate or deactivate Trend Micro's own Firewall and Behavior Monitoring features in the same way.

### Malware alerts

The following alert is shown in the browser if the user attempts to download the EICAR test file:



Website blocked by Trend Micro Worry-Free Business Security Services

Malicious website blocked

http://www.eicar.org/download/eicar.com

**Rating:** Dangerous Verified fraudulent page or threat source.

What You Can Do:

- Contact your administrator about security settings on your network
- I understand the risks and I want to continue browsing

Copyright © 2015. Trend Micro Incorporated. All rights reserved.

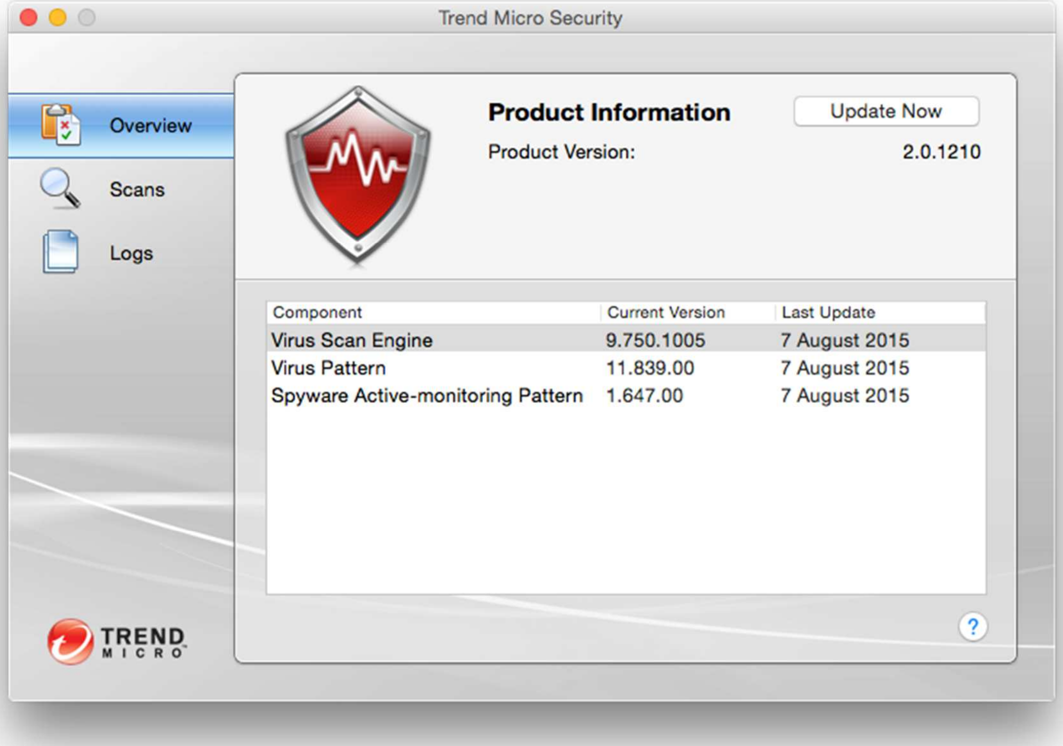
## Windows server protection software

In terms of user interface and accessible functions, the server protection software can be regarded as identical to that for the client.

### Comment

Overall, we found the Windows protection software to be very simple to use, with all the essential features easily accessible. We were however surprised to see that by default, standard users can disable the agent completely. This can be password protected from the console; we strongly advise admins to do this.

## Mac client protection software



**Product Information**

Product Version: 2.0.1210

| Component | Current Version | Last Update |
|---|---|---|
| Virus Scan Engine | 9.750.1005 | 7 August 2015 |
| Virus Pattern | 11.839.00 | 7 August 2015 |
| Spyware Active-monitoring Pattern | 1.647.00 | 7 August 2015 |

### Installation

Common Tasks/Add Devices in console; the setup wizard lets the administrator choose the drive and folder to install the program to, but otherwise there are no choices to be made.

### Main program window

The *Overview* tab of the main window shows the current version of major components and provides an *Uptdate Now* button. The *Scans* button allows the user to run quick, full and custom scans, whilst logs and quarantine can be accessed from the *Logs* button. The *?* symbol opens the local help window.

### System Tray icon

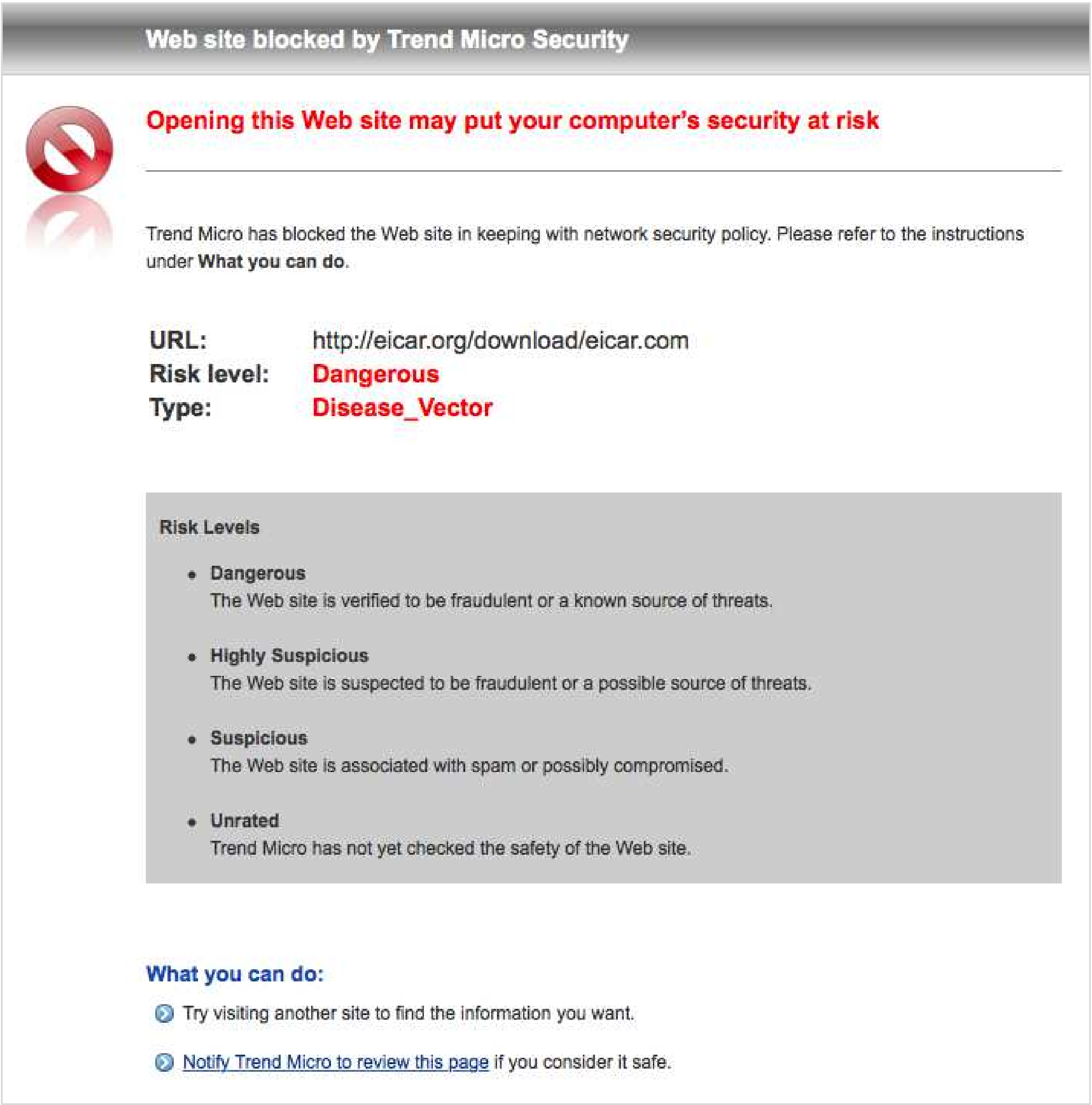
There is a system tray icon, from which the user can open the program or run an update.

### Unauthorised access

There is no means of deactivating protection from the client, regardless of the user account type.

### Malware alerts

If the user attempts to download the EICAR test file, the following alert is shown in the browser window:



Web site blocked by Trend Micro Security

Opening this Web site may put your computer's security at risk

Trend Micro has blocked the Web site in keeping with network security policy. Please refer to the instructions under **What you can do**.

| | |
|---|---|
| URL: | http://eicar.org/download/eicar.com |
| Risk level: | Dangerous |
| Type: | Disease_Vector |

Risk Levels

- **Dangerous**
  The Web site is verified to be fraudulent or a known source of threats.
- **Highly Suspicious**
  The Web site is suspected to be fraudulent or a possible source of threats.
- **Suspicious**
  The Web site is associated with spam or possibly compromised.
- **Unrated**
  Trend Micro has not yet checked the safety of the Web site.

**What you can do:**

- Try visiting another site to find the information you want.
- Notify Trend Micro to review this page if you consider it safe.

## Comment

The Mac client protection software is very simple, with all the essential functions very easy to find. Users can run updates and scans, but not disable the protection.

## Summary

We found Trend Micro's cloud console to be very well laid-out and easy to navigate. System status is displayed every time the admin logs on, and any problems shown can be resolved directly from the same page. The *Devices* view presents a clear overview of clients, and makes everyday administration tasks, such as running scans, intuitive and straightforward. Client software is simple and easy to use. We do however feel that the current help facilities for the console are very basic and could be improved.

| | Bitdefender Endpoint GravityZone | ESET Remote Administrator | F-Secure Protection Service for Business | G DATA AntiVirus Business | Kaspersky Small Office Security | McAfee SaaS Endpoint Protection | Sophos Endpoint Security and Control Cloud | Symantec Endpoint Protection | Trend Micro Worry-Free Business Security Services |
|---|---|---|---|---|---|---|---|---|---|
| **Console type and features** | | | | | | | | | |
| **Console type** | | | | | | | | | |
| Cloud-based console | ● | | ● | ● | ● | ● | ● | | ● |
| On-premise Windows-based console | N/A | ● | | ● | | ● | ● | ● | N/A |
| On-premise virtual appliance | ● | ● | | ● | | ● | ● | | N/A |
| **Minimum hardware requirements for Windows-based console** | | | | | | | | | |
| CPU (GHz) | 2x2GHz | 2x2GHz | | 2GHz | N/A | N/A | 1GHz | | N/A |
| RAM (GB) | 4 GB | 3 GB | | 1 GB | N/A | N/A | 512MB | 2 GB | N/A |
| **Supported virtualisation systems for virtual appliances** | | | | | | | | | |
| VMware vSphere | ● | ● | | ● | N/A | ● | ● | | N/A |
| VMware ESXi | ● | ● | | ● | N/A | ● | ● | ● | N/A |
| VMware Workstation | ● | ● | | ● | N/A | ● | | ● | N/A |
| VMware Player | ● | ● | | ● | N/A | ● | | | N/A |
| Oracle Virtual Box | ● | ● | | ● | N/A | | | ● | N/A |
| Microsoft Hyper-V | ● | ● | | ● | N/A | ● | ● | ● | N/A |
| Citrix Xen Server | ● | | | ● | N/A | | | ● | N/A |
| Citrix Xen Desktop | ● | | | ● | N/A | | | | N/A |
| **Client software deployment methods** | | | | | | | | | |
| Push installation from the console | ● | ● | | ● | | | ● | ● | |
| Email a link to remote users to install the software themselves | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Creation of .exe or .msi installer package | ● | | ● | ● | | ● | ● | ● | ● |
| **Client management actions that can be run from the console** | | | | | | | | | |
| Update signatures | ● | ● | | ● | ● | ● | ● | ● | ● |
| Reboot computer | ● | ● | | | | ● | | ● | |
| Scan computer | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Enable/Disable On-Access Scan and/or Firewall | ● | ● | ● | ● | ● | ● | ● | ● | ● |

**Supported Server OS**

| Microsoft Windows servers | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Windows Server 2003/2008 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| Windows Server 2003 R2 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| Windows Server 2008/2012 R2 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| Windows Server 2012 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| Windows Small Business Server 2003 32-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | | N/A | ● | N/A | ● | | | N/A | ● |
| Windows Small Business Server 2003 R2 32-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | | N/A | ● | N/A | ● | | | N/A | ● |
| Windows Small Business Server 2008 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | | N/A | ● |
| Windows Small Business Server 2011 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| Windows Server 2012 Essentials 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| Windows Server 2012 R2 Essentials 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |

**Supported Desktop OS**

| Microsoft Windows clients | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Windows XP** | | | | | | | | | | | | | | | | | | |
| Home/Media Center | N/A | ● | | ● | N/A | | ● | ● | N/A | | N/A | | N/A | ● | | | N/A | ● |
| Professional 32-bit | N/A | ● | | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| Professional 64-bit | N/A | ● | | ● | N/A | | ● | | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| **Windows Vista** | | | | | | | | | | | | | | | | | | |
| Home Basic/Home Premium 32-bit / 64-bit | N/A | ● | | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | ● | N/A | ● |
| Business/Enterprise/Ultimate 32-bit / 64-bit | N/A | ● | | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | ● | N/A | ● |
| **Windows 7** | | | | | | | | | | | | | | | | | | |
| Starter Edition | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | | N/A | ● |
| Home Premium 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| Professional/Ultimate/Enterprise 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | | N/A | ● |
| **Windows 8** | | | | | | | | | | | | | | | | | | |
| Consumer version 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | | N/A | ● |
| Professional/Enterprise 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| **Windows 8.1** | | | | | | | | | | | | | | | | | | |
| Consumer version 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | | N/A | ● |
| Professional/Enterprise 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● |
| **Windows 10** | | | | | | | | | | | | | | | | | | |
| Home 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | | N/A | ● |
| Pro/Education/Enterprise 32-bit / 64-bit | N/A | ● | ● | ● | N/A | ● | ● | ● | N/A | ● | N/A | ● | N/A | ● | | ● | N/A | ● |

| Apple Mac OS clients | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client | Management Console | Protection client |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| OS X 10.7 | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● | N/A | | N/A | ● | N/A | | N/A | ● |
| OS X 10.8 and higher | N/A | ● | N/A | ● | N/A | ● | ● | ● | N/A | ● | N/A | | N/A | ● | N/A | ● | N/A | ● |

| | Bitdefender Endpoint GravityZone | ESET Remote Administrator | F-Secure Protection Service for Business | G DATA AntiVirus Business | Kaspersky Small Office Security | McAfee SaaS Endpoint Protection | Sophos Endpoint Security and Control Cloud | Symantec Endpoint Protection | Trend Micro Worry-Free Business Security Services |
|---|---|---|---|---|---|---|---|---|---|
| **Supported Mobile OS** | | | | | | | | | |
| **Google Android clients** | | | | | | | | | |
| 4.4 - 5.1.1 | | ● | ● | ● | ● | | ● | | ● |
| **Apple iOS clients** | | | | | | | | | |
| 6.0 - 6.1 | | | | | | | ● | | ● |
| 7.0 - 9.0 | | | ● | ● | | | ● | | ● |
| **Client-Software Features** | | | | | | | | | |
| **Microsoft Windows clients** | | | | | | | | | |
| Antimalware | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Antispam | ● | ● | ● | ● | ● | ● | ● | | ● |
| Data backup | | ● | | ● | ● | | | | |
| Data encryption | | ● | | | ● | ● | ● | | |
| Device control | ● | ● | | ● | ● | | ● | ● | ● |
| Firewall | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Phishing protection | ● | ● | ● | ● | ● | ● | ● | | ● |
| Settings protection* | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Theft protection | | | | | ● | | ● | | |
| Uninstall protection** | ● | ● | | ● | ● | ● | ● | ● | ● |
| Web access control | ● | ● | ● | ● | ● | ● | ● | | ● |
| **Apple Mac OS clients** | | | | | | | | | |
| Antimalware | ● | ● | ● | ● | ● | | ● | ● | ● |
| Antispam | | | | | | | ● | | |
| Data encryption | | | | | | | ● | | |
| Device control | | ● | | | | | ● | | |
| Firewall | | ● | | | | | ● | | |
| Phishing protection | ● | ● | | ● | ● | | ● | | ● |
| Settings protection* | ● | ● | | | ● | | ● | ● | ● |
| Theft protection | | | | | ● | | ● | | |
| Uninstall protection** | | ● | | | ● | | ● | ● | ● |
| Web access control | | ● | | | ● | | ● | | ● |
| **Google Android clients** | | | | | | | | | |
| Antimalware | | ● | ● | ● | ● | | ● | N/A | ● |
| App control | | ● | ● | ● | | | ● | N/A | |
| Call/text-message blocker | | ● | ● | ● | ● | | | N/A | |
| Phishing protection | | ● | ● | ● | ● | | ● | N/A | ● |
| Settings protection* | | ● | | | ● | | ● | N/A | ● |
| Theft protection | | ● | ● | ● | ● | | ● | N/A | ● |
| Uninstall protection** | | ● | | | ● | | ● | N/A | |
| Web access control | | | | | | | ● | N/A | ● |
| **Apple iOS clients** | | | | | | | | | |
| Antimalware | | | | | | | ● | N/A | |
| App control | | | | ● | | | ● | N/A | |
| Phishing protection | | | ● | | | | ● | N/A | |
| Settings protection* | | | | ● | | | ● | N/A | ● |
| Theft protection | | | ● | ● | | | ● | N/A | ● |
| Uninstall protection** | | | | | | | ● | N/A | |
| Web access control | | | | | | | ● | N/A | |
| **General** | | | | | | | | | |
| **Support** | | | | | | | | | |
| Telephone support | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| Remote control by support staff available | ● | ● | ● | ● | | ● | ● | ● | ● |
| Email support | ● | ● | ● | ● | ● | ● | ● | | ● |
| Support forum | | ● | ● | ● | ● | ● | ● | ● | |
| Chat support | ● | | ● | ● | | ● | ● | | ● |
| **Languages:** | | | | | | | | | |
| Which languages can be used to contact support? | English, Spanish, German, Romanian, French, Malay, Bengali, Portuguese | All | English, Japanese, French, Danish, Finnish, German, Norwegian, Swedish | German, English, Italian, Spanish, French | English, Russian, German, French, Spanish, Italian, Portuguese, Polish, Arabic, Turkish, Czech, Hungarian, Dutch, Chinese | Chinese, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish | English, French, German, Italian, Japanese, Spanish, Chinese | English, Portuguese, French, Italian, German, Spanish, Chinese, Japanese, Korean | English, German, French, Italian, Spanish, Portuguese, Japanese, Chinese, Russian, Polish, Dutch, Danish, Norwegian, Swedish |
| Which interface languages is the product available in? | English, Spanish, German, Romanian, French, Polish | English, German, Spanish, French, Russian, Polish, Italian, Japanese, Chinese, Arabic, Slovak, Czech, Croatian, Korean | English, Czech, Danish, Dutch, Estonian, Finnish, French, German, Greek, Hungarian, Italian, Japanese, Korean, Norwegian, Polish, Portuguese, Romanian, Russian, Slovenian, Spanish, Swedish, Turkish, Chinese | German, English, Italian, Spanish, French, Russian, Polish, Turkish, Portuguese, Chinese | English, Russian, German, French, Spanish, Italian, Portuguese, Polish, Arabic, Turkish, Czech, Hungarian, Dutch, Chinese | Chinese, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish | English, French, German, Italian, Japanese, Spanish, Chinese | Portuguese, Chinese, Czech, English, French, German, Italian, Japanese, Korean, Spanish, Polish, Russian | English, German, French, Italian, Spanish, Portuguese, Japanese, Chinese, Russian, Polish, Dutch, Danish, Norwegian, Swedish |
| Which languages are the manuals available in? | English, Spanish, German, Romanian, French, Polish | English, German, Spanish, French, Russian, Polish, Italian, Japanese, Chinese, Arabic, Slovak, Czech, Croatian, Korean | English, German, Spanish, Finnish, French, Italian, Japanese, Swedish | German, English, French, Polish, Chinese | English, Russian, German, French, Spanish, Italian, Portuguese, Polish, Arabic, Turkish, Czech, Hungarian, Dutch, Chinese | Chinese, Danish, Dutch, English, Finnish, French, German, Italian, Japanese, Korean, Norwegian, Portuguese, Russian, Spanish, Swedish, Turkish | English, French, German, Italian, Japanese, Spanish, Chinese | Portuguese, Chinese, Czech, English, French, German, Italian, Japanese, Korean, Spanish, Polish, Russian | English, German, French, Italian, Spanish, Portuguese, Japanese, Chinese, Russian, Polish, Dutch, Danish, Norwegian, Swedish |
| **Pricing (approximate prices according to vendor, as of September 2015)** | | | | | | | | | |
| **5 clients and 1 file server** | | | | | | | | | |
| 1 year $ USA | 141 | 170 | 440 | 213 | 150 | 179 | 244 | 257 | 189 |
| 3 years $ USA | 282 | 356 | 1.100 | 426 | 300 | 312 | 488 | 341 | 415 |
| 1 year € DE | 168 | 151 | 440 | 213 | 200 | 179 | 214 | 278 | 232 |
| 3 years € DE | 336 | 316 | 1.100 | 426 | 448 | 312 | 428 | 366 | 696 |
| **25 clients and 1 file server** | | | | | | | | | |
| 1 year $ USA | 565 | 532 | 1.606 | 702 | 600 | 750 | 731 | 928 | 944 |
| 3 years $ USA | 1.130 | 1.117 | 4.015 | 1.404 | 1.200 | 1.312 | 1.487 | 1.369 | 2.076 |
| 1 year € DE | 672 | 473 | 1.606 | 702 | 886 | 750 | 656 | 1.116 | 833 |
| 3 years € DE | 1.346 | 993 | 4.015 | 1.404 | 1.993 | 1.312 | 1.312 | 1.649 | 2.499 |

N/A: not applicable. In the case of a cloud-based console, there is nothing to be installed; a virtual appliance is delivered with its own operating system.

*Admin can prevent users changing settings

**Admin can prevent users uninstalling the product

## Copyright and Disclaimer

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 2015)