Anti-Virus Comparatives

Review of Business Disk-Encryption Products

Language: English
December 2016

Last Revision: 17th March 2017

www.av-comparatives.org

Commissioned by ESET

Table of Contents

Introduction

Encryption of system drives and removable media is a very important security consideration for businesses large and small. If an encrypted device is lost or stolen, the data contained on it cannot be read without the appropriate password or encryption key, meaning that confidential business information remains safe. Using data encryption software, it is possible to encrypt the entire hard drive/solid state drive of a laptop or desktop computer, meaning that even if a thief physically removes the system drives and connects it to another computer, they will not be able to access any data or system files on it. Removable media encryption is another important feature of encryption software, meaning that e.g. a flash drive containing a business presentation can only be accessed by entering a password or encryption key. Finally, encryption of individual files and folders can be a simple means of granting selective access to company data.

This review covers 5 mainstream encryption products for business. We have considered the range of features available, i.e. full disk/removable media/selected file and folder/email encryption; the ease of installation and use of the product; suitability for businesses of all sizes; manageability.

Products reviewed

Please note that we used the latest version of each product available at the time of the review (December 2016).

- **ESET DESlock+ Pro**, with DESlock+ Enterprise Server 2.7.1 and DESlock+ Client 4.8.11
- **McAfee Drive Encryption** 7.1.0 with McAfee ePolicy Orchestrator 5.1.0
- **Microsoft BitLocker** for Windows 10 Enterprise, Version 1607 (Build 14393.447)
- **Sophos SafeGuard**, with SafeGuard Management Center 8.00.2.13 and Sophos SafeGuard client software 8.00.0.251
- **Symantec Endpoint Encryption** 11.1.0

Management Summary

ESET DESlock+ stands out for a number of reasons. Firstly, the management console can be installed on any supported Windows client or Windows Server operating system, in either a workgroup or domain setup. This makes it particularly suitable for smaller businesses without Active Directory or a Windows Server machine. Secondly, the management server is very simple to set up, as the installation wizard automatically installs any prerequisite software, without the administrator having to do anything. No expertise in prerequisite software (e.g. SQL Server or Internet Information Services) is required. Again, this makes it ideal for smaller businesses without experienced, full-time IT staff. The management console has a very clean, simple layout, making it easy to find essential features and information. Users can manage encryption of their own removable media and files/folders using a very straightforward GUI on client PCs. DESlock+ is also notable for its full range of functionality, providing not only full HDD/SSD encryption, but full and partial encryption options for removable media, plus encryption of individual files and folders, and email encryption too. Recovery options include two different methods for recovering encrypted data from an unbootable computer.

Microsoft BitLocker in Windows 10 has two distinct plus points: firstly, it is free, and secondly it is already integrated into the operating system, so no installation or configuration is required. Its functionality is accessed using Windows Explorer, and the functions it has are easy to use. However, it has the major drawback that there is no central management. Administrators must make and update lists of encryption keys and the machines they belong to. To manage remote users, administrators would need to use remote control software to perform tasks themselves, or provide users with instructions for this. There is also the question of securely transferring encryption keys from remote users to the administrator for backup purposes. BitLocker does not allow for partial encryption of removable media, or the encryption of individual files and folders. Small businesses using the Home edition of Windows 10 should note that BitLocker is not included in this variant.

McAfee Drive Encryption requires the separate installation of the ePolicy Orchestrator management console on the server, and local installation of the management agent on the clients. However, we found installing these, and the Drive Encryption management server, to be very straightforward. Deployment of the clients is by remote push installation from the console, which again was unproblematic. Readers should note that McAfee Drive Encryption only covers system drives, and does not allow encryption of removable media devices, or specific files and folders. Although Active Directory is not required, the ePolicy Orchestrator management console has to be installed on a Windows Server operating system.

Sophos SafeGuard provides managed encryption of system drives, removable media and individual files and folders. Although it does not require Active Directory, the console has to be installed on a Windows Server operating system. Installing and configuring the product requires some experience of Microsoft SQL Server and Internet Information Services, and the use of policies as typically found in enterprise endpoint protection software. This makes it better suited to larger companies with experienced, full-time IT staff.

Symantec Endpoint Encryption allows the encryption of system drives and removable media. It requires an Active Directory domain and is thus unsuitable for small businesses with workgroup configurations. Installation of the product requires experience of installing and configuring Microsoft SQL Server and Internet Information Services.

Feature table

All the participating products offer full disk encryption. In the table below we have indicated whether the products additionally allow full and/or partial encryption of USB devices, encryption of individual files and folders, a "digital shredder" (secure file deletion) and email encryption.

Product	Management console	USB Device Complete Encryption	USB Device Selected Encryption	File and folder encryption	Digital Shredder	Email encryption
ESET	Yes	Yes	Yes	Yes	Yes	Yes
McAfee	Yes	No	No	No	No	No
Microsoft	No[1]	Yes	No	No[2]	No	No
Sophos	Yes	Yes	No	Yes[3]	No	No
Symantec	Yes	Yes	Yes	Yes	No	No

Suitability for use in businesses of all sizes

All of the products in this review can be used in corporate environments with Windows Server operating systems and an Active Directory domain. The table below shows whether the system requirements make the product suitable for smaller businesses as well. Very small businesses will use a workgroup setup with Windows client operating systems only, and so will require a solution compatible with this setup. Many slightly larger companies that do use an Active Directory domain will not have full-time professional IT staff, and so need a product that can be installed without any specialist knowledge of e.g. Microsoft SQL Server or Windows Internet Information Services.

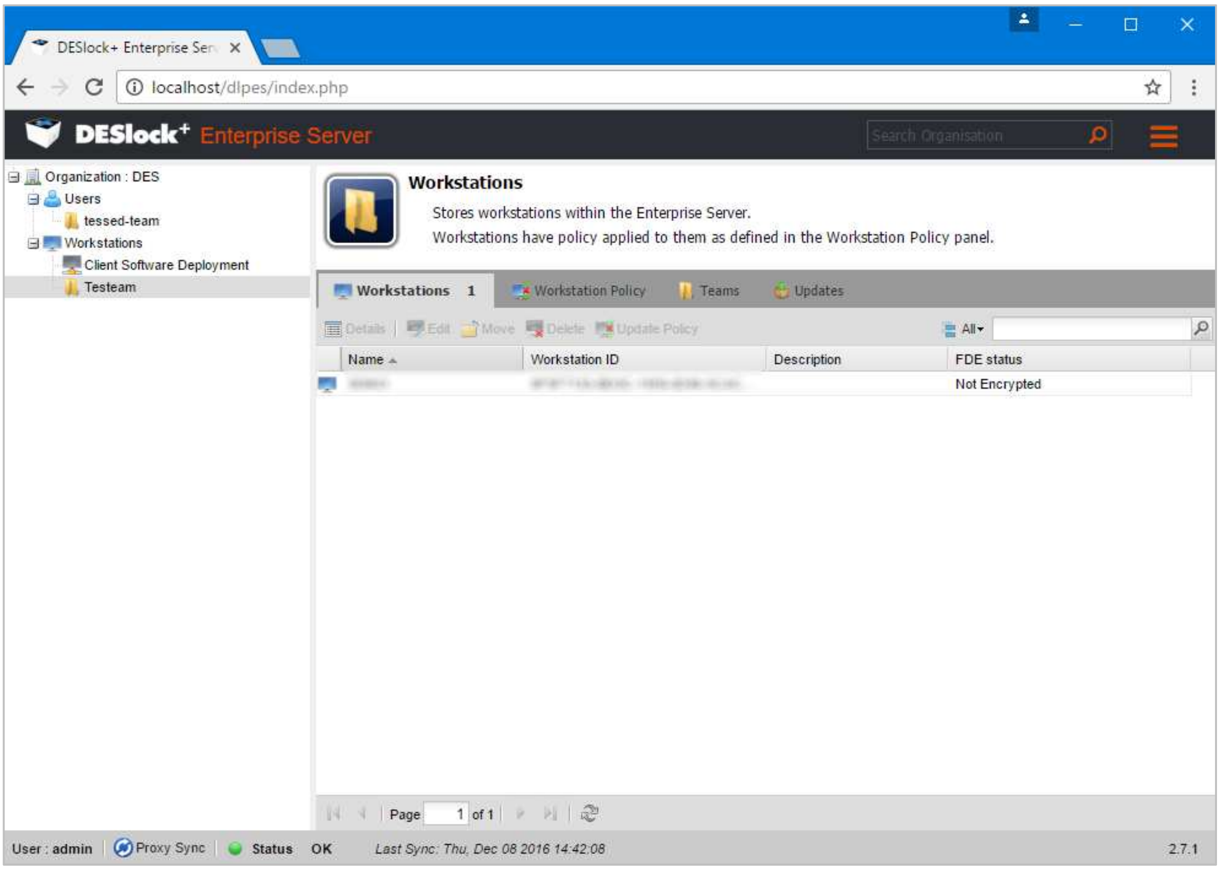
Product	Server OS required	AD required	Manual installation/configuration of prerequisite software required
ESET	No	No	No
McAfee	Yes	No	No
Microsoft	No	No	No
Sophos	Yes	No	Yes
Symantec	Yes	Yes	Yes

[1] Microsoft BitLocker Administration and Monitoring (MBAM) is available from Microsoft to manage BitLocker. However, readers should note that (a) this is a paid-for option, and (b) that it requires the use of, and expertise in, additional Microsoft software such as SQL server, System Center Configuration Manager, Active Directory, and Internet Information Services.

[2] Microsoft's Encrypting File System (EFS) is built into Windows, and allows encryption of individual files and folders. However, it is entirely separate from BitLocker and controls access to encrypted files using Windows user accounts.

[3] "Encrypt according to policy"

ESET DESlock+ Pro



Workstations

Stores workstations within the Enterprise Server.
Workstations have policy applied to them as defined in the Workstation Policy panel.

Name	Workstation ID	Description	FDE status
[redacted]	[redacted]		Not Encrypted

Last Sync: Thu, Dec 08 2016 14:42:08

Overview

Product version reviewed

DESlock+ Enterprise Server 2.7.1

DESlock+ Client 4.8.11

Windows operating systems supported

Clients: Windows XP, Vista, 7, 8, 8.1, 10

Servers: Windows Server 2003 - 2012

The DESlock+ Pro management console can be installed on any supported client or server operating system. Active Directory is not required.

Other supported platforms

DESlock+ also supports iOS devices (not covered in this review).

About the product

ESET DESlock+ Pro provides centrally managed encryption software for Windows servers and workstations. It allows the encryption of complete system drives, virtual disks, removable media drives, individual files and folders, plus text and clipboard contents. A server-based central management console allows the administrator to monitor and manage encryption on all systems from a single location. The console is capable of managing multiple organizations, including multiple Active Directory domains and locations. However, because it does not require a Windows Server operating system or an Active Directory domain, it is equally suited to a small business with a single location and domain or workgroup.

Additional features

The DESlock+ Pro client software includes a digital shredder, meaning that users can securely delete sensitive files and folders on their PCs. A cloud proxy server makes settings and updates available to clients without the security risk of opening ports on the management server.

Product page on vendor's website

https://www.eset.com/int/business/endpoint-security/encryption-deslock/

What we liked about the product

ESET DESlock+ provides a full range of encryption options, covering full disk, file/folder and removable media encryption, with management from a central console.

The product is well suited to small businesses as well as corporations. The flexible technical requirements of the management console mean that it can run equally well on a Windows client OS in a workgroup as on a Windows Server computer in an Active Directory domain.

The management server can be set up using a single installation wizard, which automatically installs any additional software components required (e.g. SQL Server). This, combined with a clean, simply laid-out console makes the product easy to use even for less-experienced administrators.

The administrator can easily assign users access to encrypted data by means of assigning encryption keys to user groups.

Intuitive client software makes it simple for users to encrypt files, folders, and removable devices on their own PCs. The addition of a new tab on the Ribbon interface of Microsoft Outlook makes encryption of emails a similarly easy task.

In a very nice touch, the recovery password generator spells out letters in the form “Alpha Bravo Charlie…” to assist admins talking to remote users on the phone.

Documentation for both the encryption software and the management console is comprehensive, very clearly laid, well-illustrated and easy to navigate.

Tips for users

Section 4 of the Enterprise Server Manual provides a clear, step-by-step guide to preparing for the deployment of client software, and we recommend users to read this first before commencing installation and deployment.

Documentation

Manuals

Separate manuals are provided for the management console and the encryption software: the 59-page DESlock+ Enterprise Server Manual, and the 35-page DESlock+ User Manual. Both provide comprehensive instructions for installing, configuring and using the products, and specific sections can easily be accessed via the clickable contents pages, bookmarks, and hyperlinks within the text itself. Both are well illustrated with appropriate screenshots.

Knowledge base

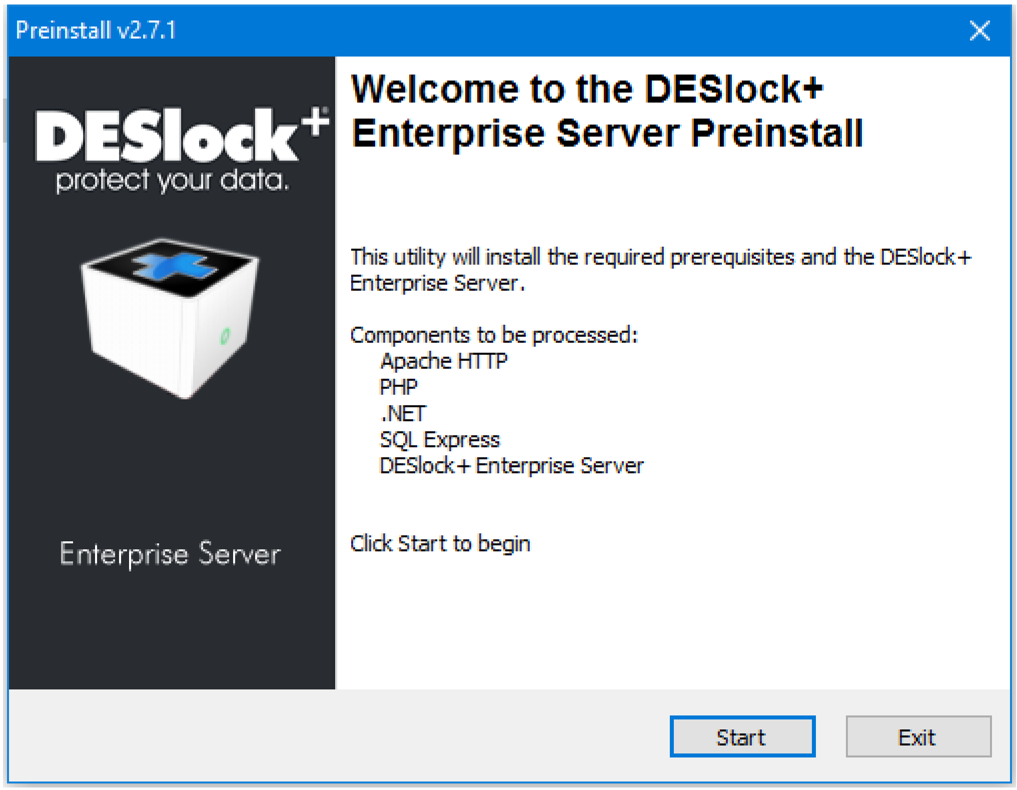
There is a searchable knowledge base on the ESET website, which provides answers to frequently asked questions for DESlock+.[4]

[4] http://support.eset.com/kb3434/

Management Console

Installation and configuration

To install the management console on the computer to be used as the management server, the administrator simply needs to run the installer file and click *Start*. Additional software components required by the console are installed automatically by the setup wizard, without any additional action being required:



Welcome to the DESlock+ Enterprise Server Preinstall

This utility will install the required prerequisites and the DESlock+ Enterprise Server.

Components to be processed:
Apache HTTP
PHP
.NET
SQL Express
DESlock+ Enterprise Server

Click Start to begin

Layout

The DESlock+ Enterprise Server console uses a very standard layout, with a left-hand pane showing an overview of items; clicking an item displays its details of in the main right-hand pane. The "tree" structure in the left-hand pane is very simple, consisting essentially of just Users and sub-groups, plus Workstations and their sub-groups. The main details pane for each item includes a row of tabs for different aspects, plus a toolbar with commonly used commands for the item in question.

The "hamburger" icon in the top right-hand corner of the console displays a menu of additional items: *Switch Organization, Control Panel, Logout, Help*.

Preparing for deployment

Section 4 of the DESlock+ Enterprise Server Manual lists the steps necessary to prepare for deployment of the encryption software to client PCs. These include creating users (identified by email address), creating groups for workstations and users, assigning policies to these, and creating customised installation packages. The process will be familiar to administrators who are used to e.g. business antivirus software management, as it follows very similar principles. Additionally, the administrator needs to create activation codes for each use, which is also explained in the manual.

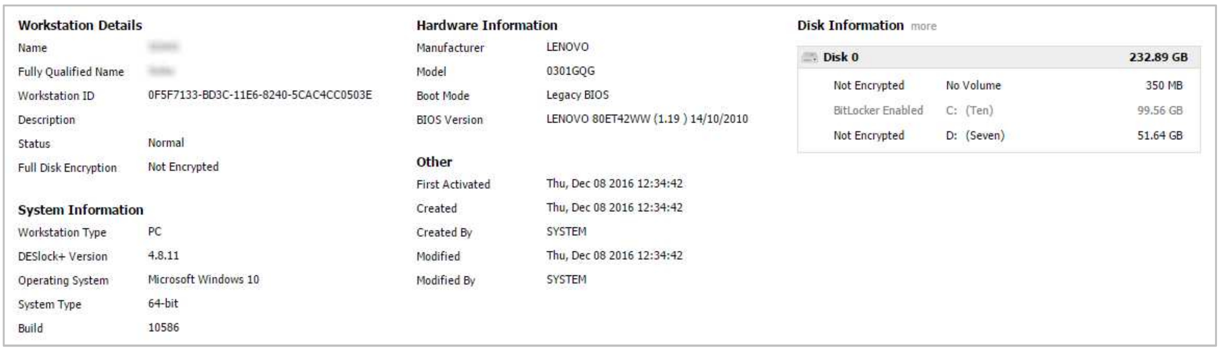
Deploying the encryption software

There are three possible methods of deploying the encryption software to client PCs, which again are very similar to those used in typical business antivirus products. The administrator can put the custom installer packages into a shared folder on the server, which can be accessed over the LAN from each client PC to be installed, or email users with an installation link. Alternatively, there is a push-installation option. We used the local installation via network share option in our test.

Monitoring the network

Workstations

Groups (*Teams*) of client PCs are shown in the console tree under *Workstations*. Clicking on the folder symbol for any team, then the *Workstations* tab, displays the workstations within that team (please see main screenshot at the start of this report). Clicking on a workstation and clicking *Details* in the toolbar displays system information for the client, including Windows version information, basic hardware details, DESlock+ version information and installation date, and disk encryption information:



Workstation Details

Name	[redacted]
Fully Qualified Name	[redacted]
Workstation ID	0F5F7133-BD3C-11E6-8240-5CAC4CC0503E
Description	
Status	Normal
Full Disk Encryption	Not Encrypted

System Information

Workstation Type	PC
DESlock+ Version	4.8.11
Operating System	Microsoft Windows 10
System Type	64-bit
Build	10586

Hardware Information

Manufacturer	LENOVO
Model	0301GQG
Boot Mode	Legacy BIOS
BIOS Version	LENOVO 80ET42WW (1.19) 14/10/2010

Other

First Activated	Thu, Dec 08 2016 12:34:42
Created	Thu, Dec 08 2016 12:34:42
Created By	SYSTEM
Modified	Thu, Dec 08 2016 12:34:42
Modified By	SYSTEM

Disk Information more

Disk 0		232.89 GB
Not Encrypted	No Volume	350 MB
BitLocker Enabled	C: (Ten)	99.56 GB
Not Encrypted	D: (Seven)	51.64 GB

The current status of the workstation is also shown. Clicking the workstation team folder, then the *Workstation Policy* tab, displays the policy settings applied to workstations in that team.

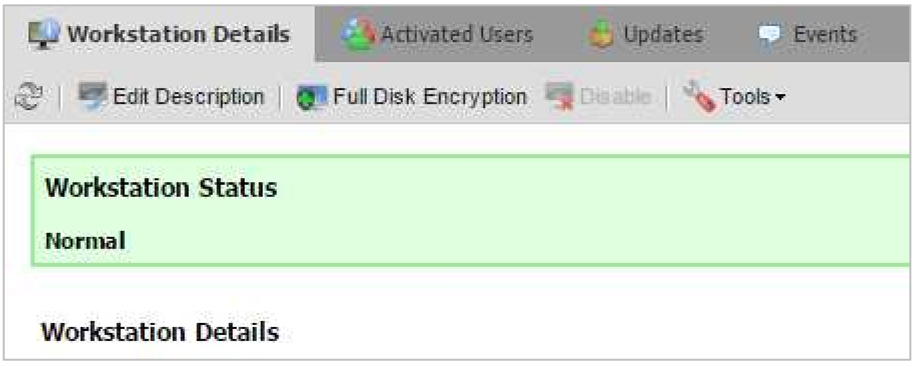
Users

User teams, individual users and user details are displayed in parallel fashion to workstations under *Users* in the console tree.

Managing the network

Full disk encryption

To encrypt a workstation's system drive, the admin accesses the *Workstation Details* for the computer in question, and clicks *Full Disk Encryption*:

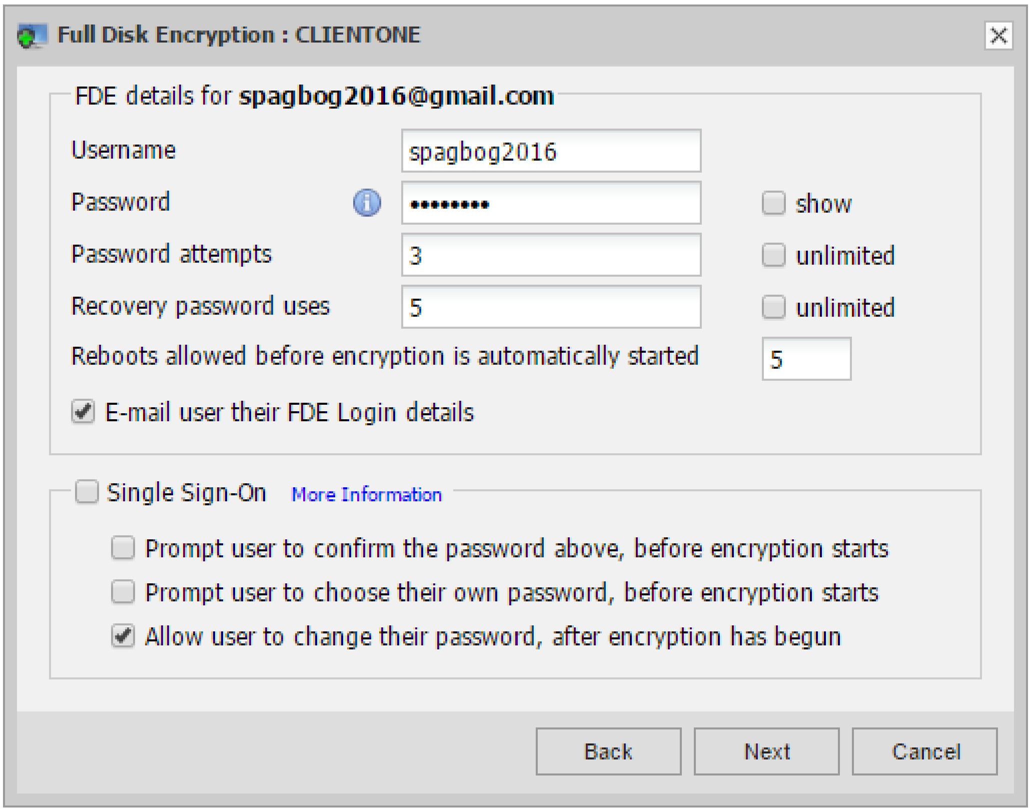


Workstation Status

Normal

Workstation Details

This starts the disk encryption wizard. A number of options are provided, including allowing the user to confirm, choose or change their passwords:



FDE details for **spagbog2016@gmail.com**

Username: spagbog2016

Password: •••••••• □ show

Password attempts: 3 □ unlimited

Recovery password uses: 5 □ unlimited

Reboots allowed before encryption is automatically started: 5

☑ E-mail user their FDE Login details

□ Single Sign-On More Information

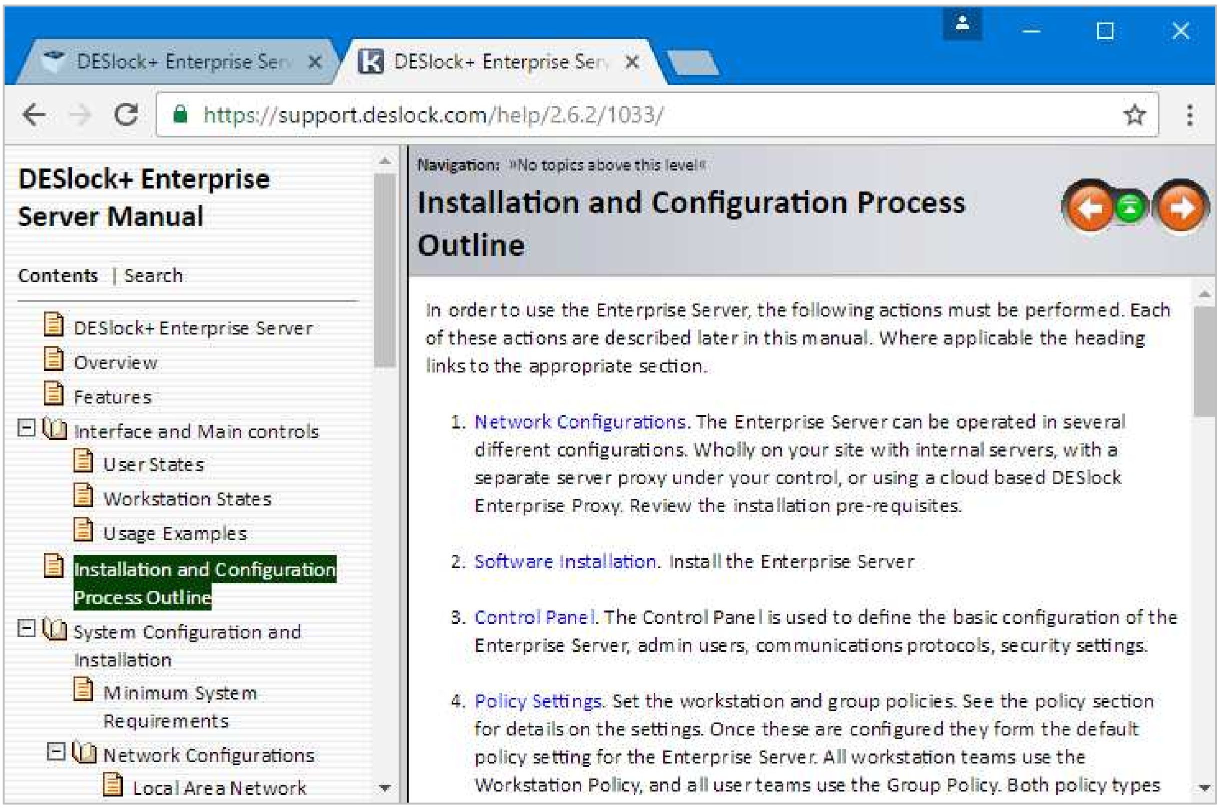
□ Prompt user to confirm the password above, before encryption starts

□ Prompt user to choose their own password, before encryption starts

☑ Allow user to change their password, after encryption has begun

Integrated help feature

Clicking the “hamburger” menu, then *Help* opens the same content as the server manual in a new browser tab:



DESlock+ Enterprise Server Manual

Contents | Search

- DESlock+ Enterprise Server
- Overview
- Features
- Interface and Main controls
  - User States
  - Workstation States
  - Usage Examples
- Installation and Configuration Process Outline
- System Configuration and Installation
  - Minimum System Requirements
  - Network Configurations
    - Local Area Network

Navigation: »No topics above this level«

Installation and Configuration Process Outline

In order to use the Enterprise Server, the following actions must be performed. Each of these actions are described later in this manual. Where applicable the heading links to the appropriate section.

1. Network Configurations. The Enterprise Server can be operated in several different configurations. Wholly on your site with internal servers, with a separate server proxy under your control, or using a cloud based DESlock Enterprise Proxy. Review the installation pre-requisites.
2. Software Installation. Install the Enterprise Server
3. Control Panel. The Control Panel is used to define the basic configuration of the Enterprise Server, admin users, communications protocols, security settings.
4. Policy Settings. Set the workstation and group policies. See the policy section for details on the settings. Once these are configured they form the default policy setting for the Enterprise Server. All workstation teams use the Workstation Policy, and all user teams use the Group Policy. Both policy types

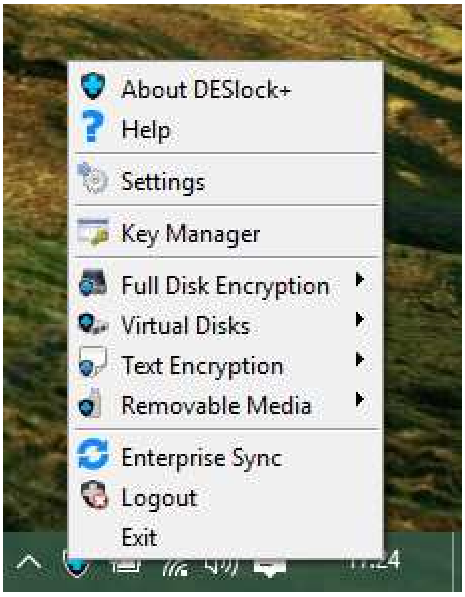
Windows client software

Installation

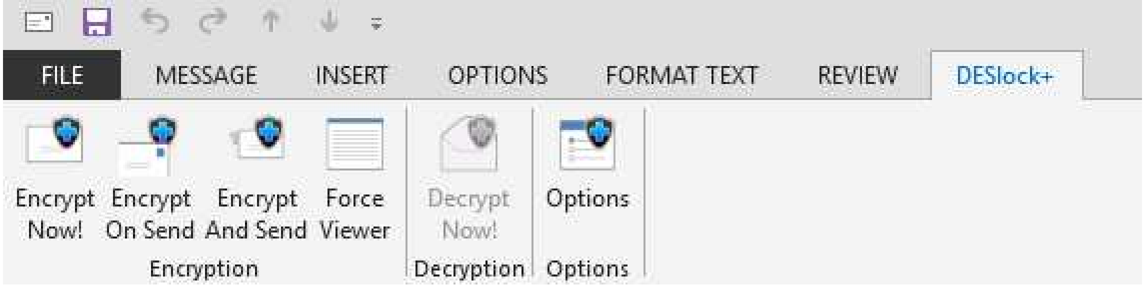
The setup wizard is very simple, and only requires the admin to accept the licence agreement, enter a user name and company name, and restart the computer at the end. After logging back on to the PC, the admin is prompted to activate the software using the key generated during preparation for deployment.

Program Interface

The main functionality of the client software is accessed by right-clicking the DESlock+ System Tray icon. This displays a menu from which the program's features can be accessed:



Additionally, a DESlock+ Ribbon Tab is added to email windows in Microsoft Outlook, to allow email encryption:

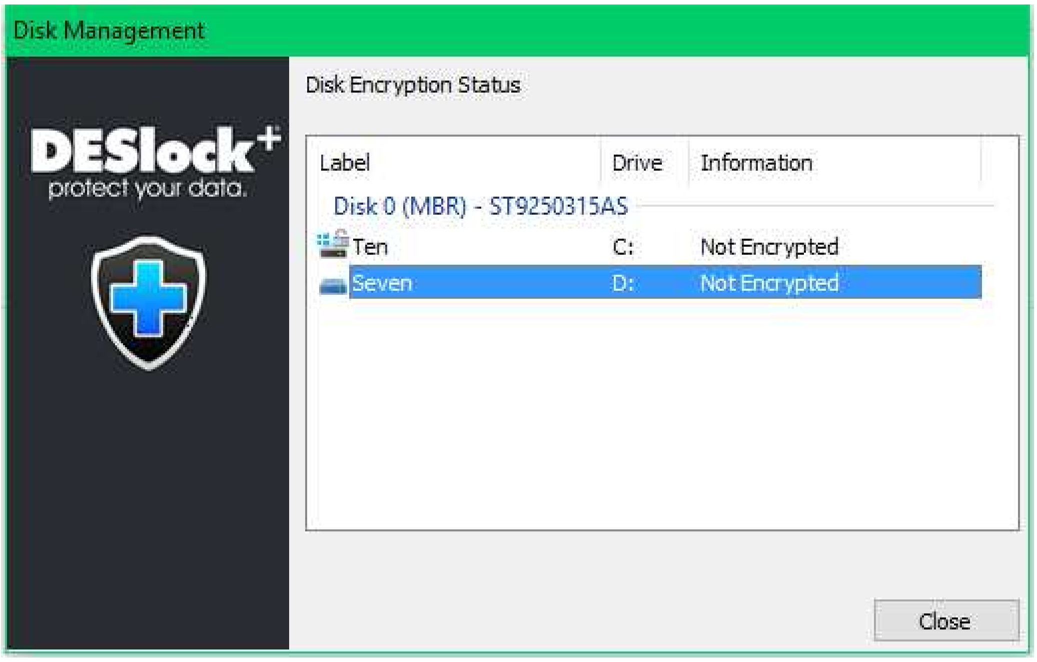


Email encryption

Emails sent from Microsoft Outlook can be encrypted using the options shown in the screenshot above.

Full disk encryption

The *Full Disk Encryption* item in the System Tray menu displays the status of full disk encryption:

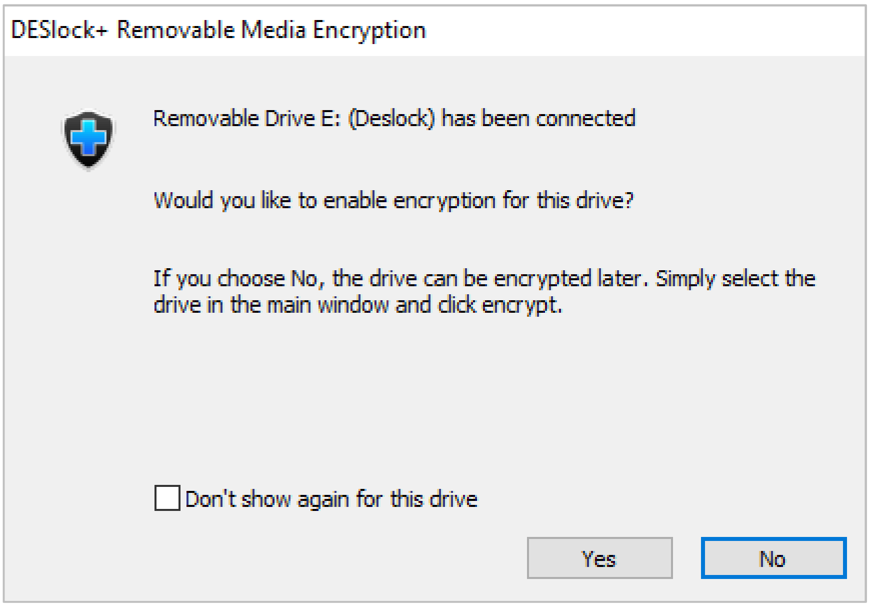


Label	Drive	Information
Disk 0 (MBR) - ST9250315AS		
Ten	C:	Not Encrypted
Seven	D:	Not Encrypted

To actually encrypt a hard disk, the administrator uses the console, as described above.

Removable media encryption

This feature can be accessed from the System Tray menu, *Removable Media*. However, when a flash drive is connected to the client PC, DESlock+ automatically prompts the user to encrypt the drive:



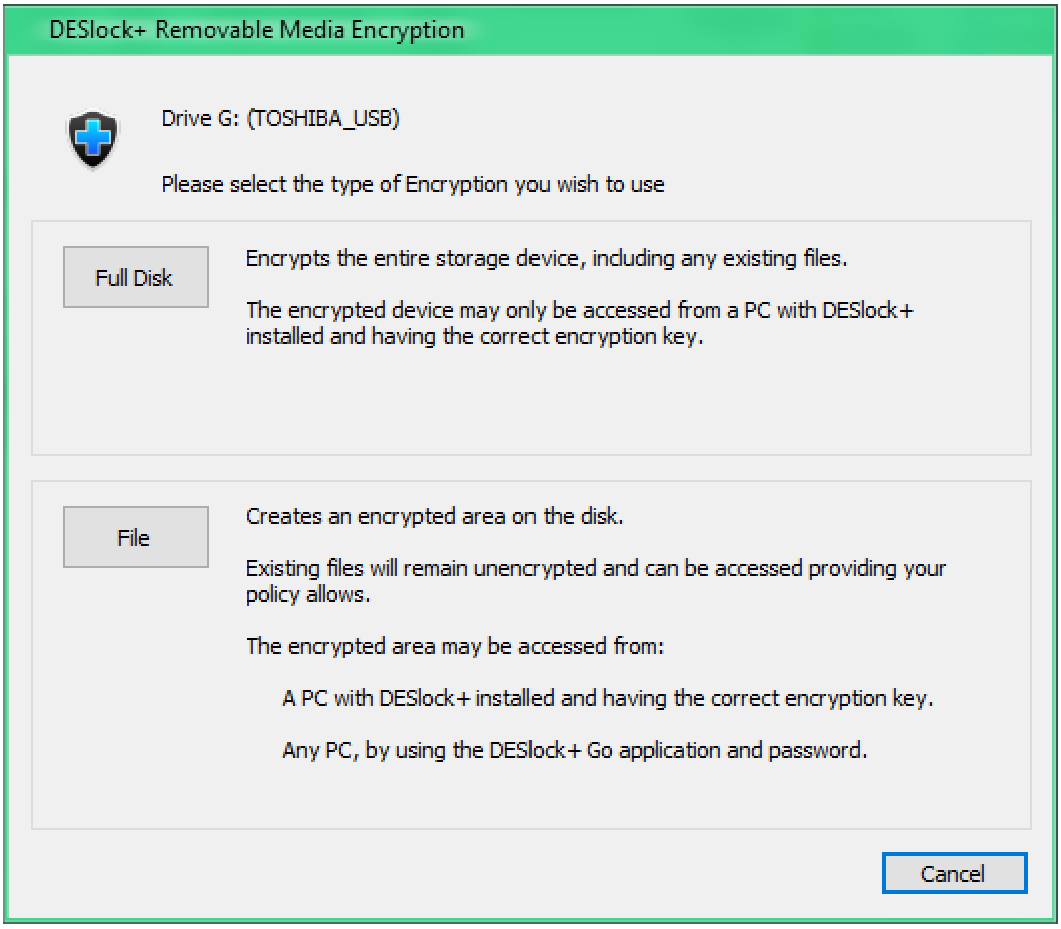
Removable Drive E: (Deslock) has been connected

Would you like to enable encryption for this drive?

If you choose No, the drive can be encrypted later. Simply select the drive in the main window and click encrypt.

☐ Don't show again for this drive

Clicking *Yes* provides the choice of Full Disk or File Encryption:



DESlock+ Removable Media Encryption

Drive G: (TOSHIBA_USB)

Please select the type of Encryption you wish to use

Encrypts the entire storage device, including any existing files.

The encrypted device may only be accessed from a PC with DESlock+ installed and having the correct encryption key.

Creates an encrypted area on the disk.

Existing files will remain unencrypted and can be accessed providing your policy allows.

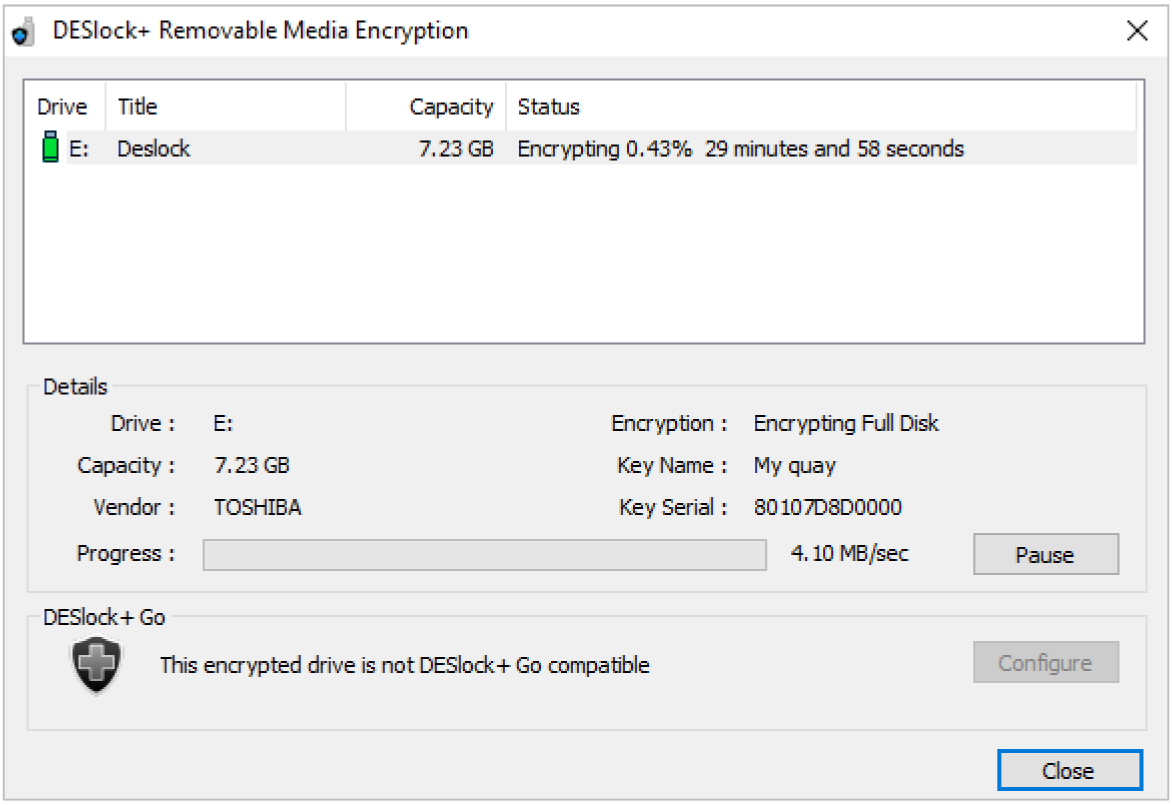
The encrypted area may be accessed from:

A PC with DESlock+ installed and having the correct encryption key.

Any PC, by using the DESlock+ Go application and password.

Full USB Drive Encryption

The screenshot below shows the progress display for Full Disk Encryption:



DESlock+ Removable Media Encryption

Drive	Title	Capacity	Status
E:	Deslock	7.23 GB	Encrypting 0.43% 29 minutes and 58 seconds

Details

Drive : E:
Capacity : 7.23 GB
Vendor : TOSHIBA
Progress : 4.10 MB/sec
Encryption : Encrypting Full Disk
Key Name : My quay
Key Serial : 80107D8D0000

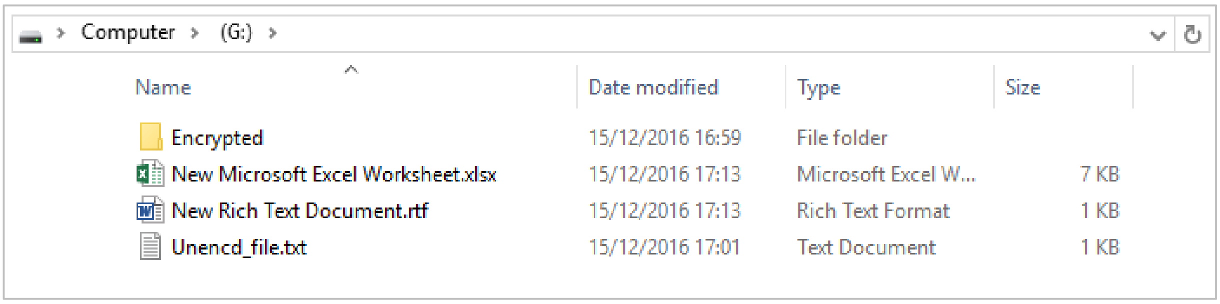
DESlock+ Go

This encrypted drive is not DESlock+ Go compatible

As noted in the setup wizard, a fully encrypted removable drive can only be accessed from a computer running the full DESlock+ program, with the appropriate encryption key.

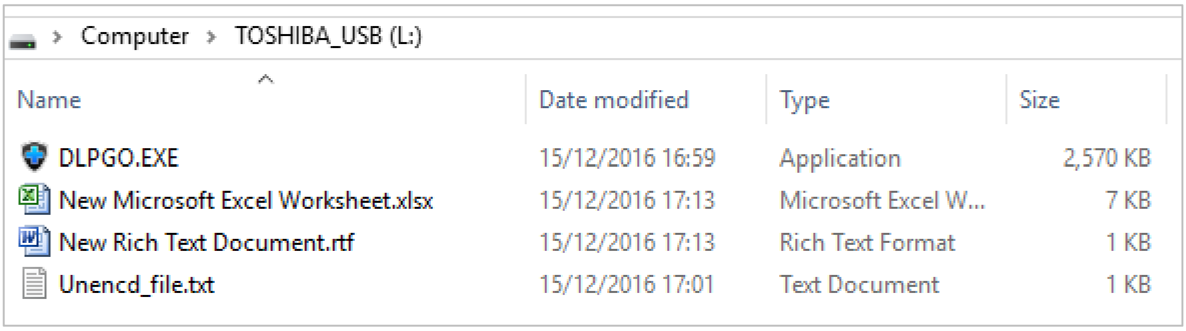
Partial USB Drive Encryption

The encryption wizard prompts the user to enter a password which will protect the encrypted files, then creates a new folder on the USB drive called “Encrypted”; files outside this folder will not be encrypted and can be accessed as normal:



Name	Date modified	Type	Size
Encrypted	15/12/2016 16:59	File folder	
New Microsoft Excel Worksheet.xlsx	15/12/2016 17:13	Microsoft Excel W...	7 KB
New Rich Text Document.rtf	15/12/2016 17:13	Rich Text Format	1 KB
Unencd_file.txt	15/12/2016 17:01	Text Document	1 KB

On another computer with the full DESlock+ program installed, the drive appears in exactly the same way as on the computer where it was encrypted. If the user has been assigned the same encryption key, he or she can open and edit files in the Encrypted folder without any further steps being required. On a computer without DESlock+ installed, the USB drive will be shown without the encrypted folder, but with the portable DESlock+ app (DLPGO.EXE) available to run:

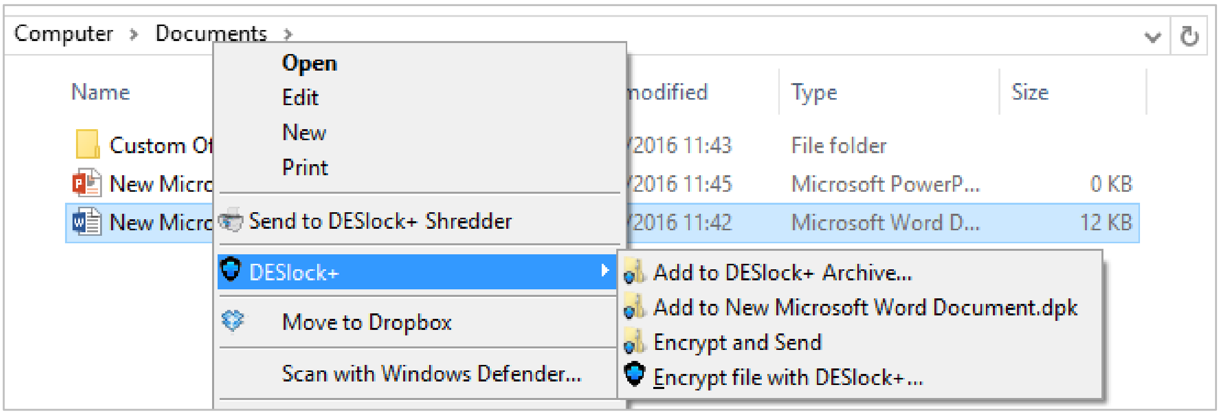


Name	Date modified	Type	Size
DLPGO.EXE	15/12/2016 16:59	Application	2,570 KB
New Microsoft Excel Worksheet.xlsx	15/12/2016 17:13	Microsoft Excel W...	7 KB
New Rich Text Document.rtf	15/12/2016 17:13	Rich Text Format	1 KB
Unencd_file.txt	15/12/2016 17:01	Text Document	1 KB

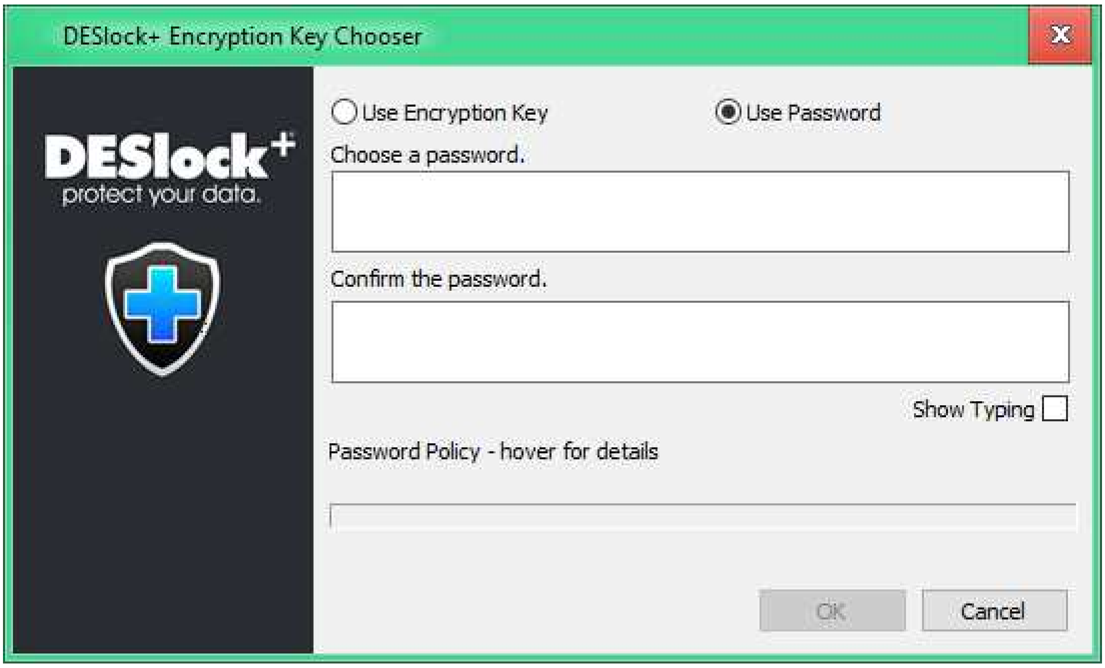
If the user executes this, the password will be requested; when this has been entered, the encrypted folder opens in a new Windows Explorer window, and files in it can be edited as normal.

File and folder encryption

To encrypt an individual file (or folder) on the local PC, the user simply right-clicks it in Windows Explorer, and chooses one of the available encryption options from the DESlock+ sub-menu. These are to add the file to an existing or new encrypted archive file; encrypt the individual file; encrypt the individual file and send it as an email attachment:



The user is provided with a choice of encryption key or password to access an encrypted file:



DESlock+ Encryption Key Chooser

○ Use Encryption Key ● Use Password

Choose a password.

Confirm the password.

Show Typing □

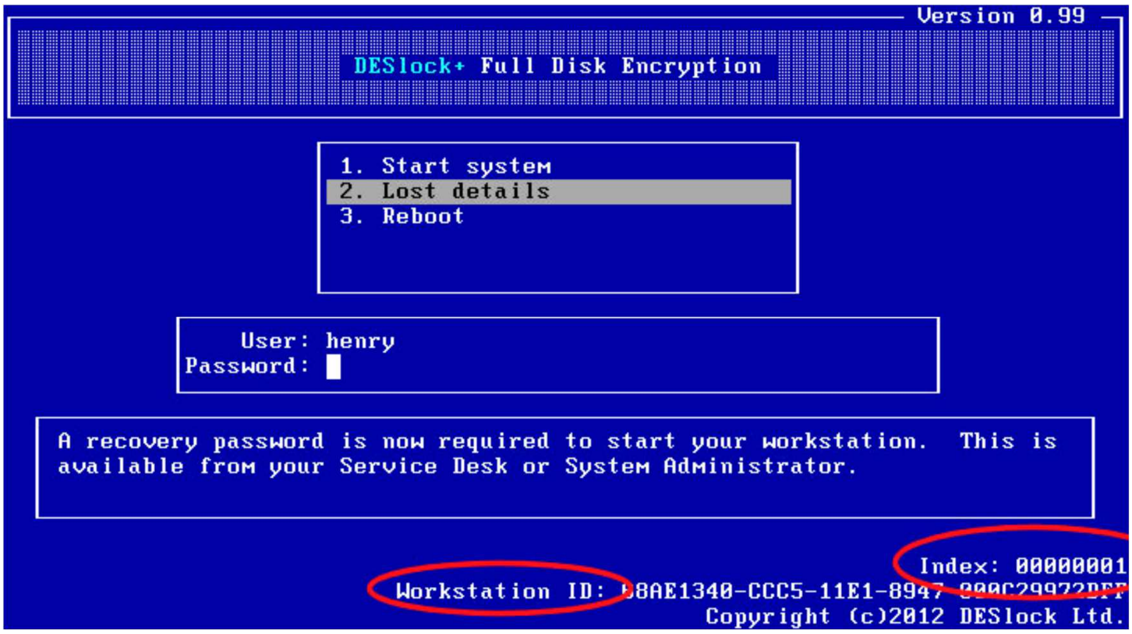
Password Policy - hover for details

In either case, the encrypted file can only be read on a PC with the full DESlock+ program installed. Choosing an encryption key means that only other users who have the same encryption key can open it; choosing a password means that only those users who know the password can open the file.

Recovery options for encrypted hard drives

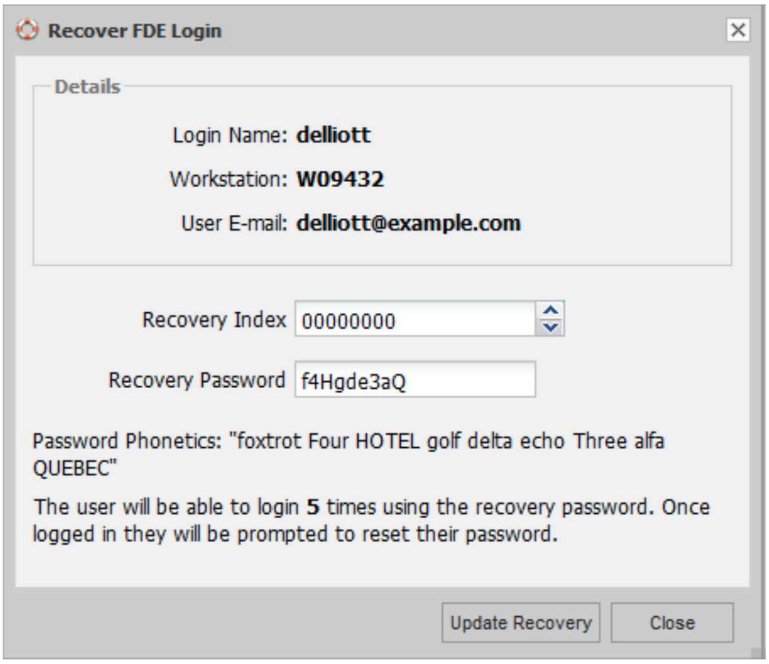
User forgets password

The DESlock+ login screen provides a *Lost details* option for the event that a user forgets their password. The user simply selects this, enters their username and presses the Enter button, and then reports the Index Number and Workstation ID (shown circled in red below) to the administrator.



```
                                                              Version 0.99
                   DESlock+ Full Disk Encryption

                      1. Start system
                      2. Lost details
                      3. Reboot

              User: henry
          Password: █

   A recovery password is now required to start your workstation.  This is
   available from your Service Desk or System Administrator.

                                                         Index: 00000001
                   Workstation ID: B8AE1340-CCC5-11E1-8947-000C29972DFF
                                            Copyright (c)2012 DESlock Ltd.
```

The admin then navigates to the correct team in the console, opens the *Details* pane for the user, and under *FDE Logins* clicks *Recover*. A recovery password, which will enable the user to log in and reset the password themselves, is generated. To aid the administrator in communicating this to the user over the phone, the developers have thoughtfully provided the “phonetic alphabet” (commonly used by police and military) version of the letters to avoid misunderstandings:



Login Name: **delliott**

Workstation: **W09432**

User E-mail: **delliott@example.com**

Recovery Index 00000000

Recovery Password f4Hgde3aQ

Password Phonetics: "foxtrot Four HOTEL golf delta echo Three alfa QUEBEC"

The user will be able to login **5** times using the recovery password. Once logged in they will be prompted to reset their password.

Recovering data from the encrypted HDD of unbootable PC

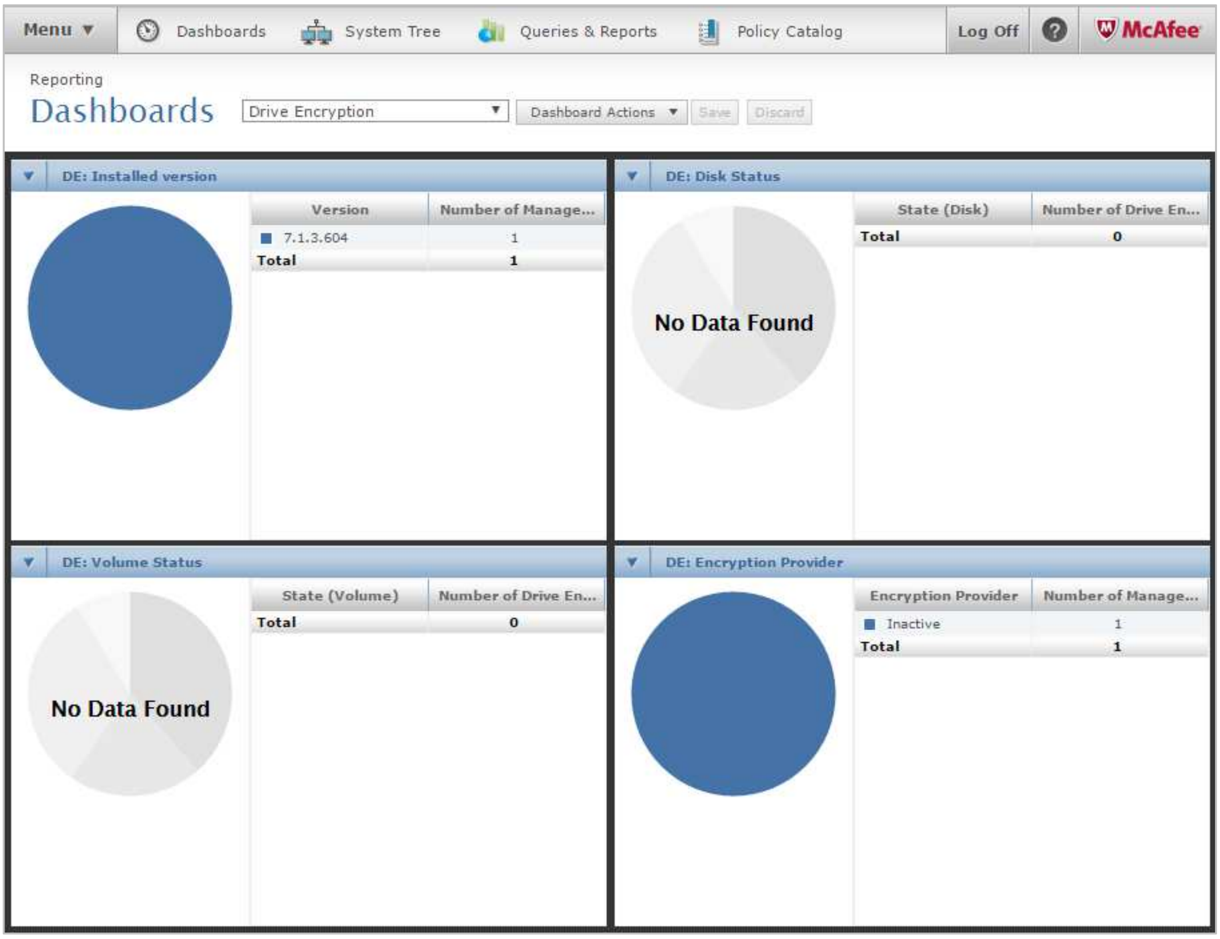
If a PC with a fully encrypted hard disk fails to boot, due to e.g. hardware failure or system file corruption, DESlock+ provides two options for recovering data from the drive. Firstly, a custom-made recovery boot disk ISO is available; the admin can burn this to CD/DVD/USB flash drive and use it to boot the PC:

https://support.deslock.com/index.php?/Default/Knowledgebase/Article/View/211

Should this not work for any reason, an alternative method, which involves booting from a standard Ubuntu Linux live disk, is available:

https://support.deslock.com/index.php?/Knowledgebase/Article/View/208/0/how-to-use-ubuntu-if-the-deslock-recovery-iso-fails

McAfee Drive Encryption



DE: Installed version

Version	Number of Manage...
■ 7.1.3.604	1
Total	1

DE: Disk Status

State (Disk)	Number of Drive En...
Total	0

DE: Volume Status

State (Volume)	Number of Drive En...
Total	0

DE: Encryption Provider

Encryption Provider	Number of Manage...
■ Inactive	1
Total	1

Overview

Product version reviewed

McAfee Drive Encryption 7.1.0

McAfee ePolicy Orchestrator 5.1.0

Windows operating systems supported

Clients: Windows XP (32-bit only); Vista, 7, 8, 8.1, 10

Servers: Windows Server 2003, 2008

The ePolicy Orchestrator console used to manage McAfee Drive Encryption can only be installed on a Windows Server operating system (2008/R2, 2012/R2). Active Directory is not required.

Other supported platforms

McAfee Drive Encryption is also supported on Apple OS X systems (not covered in this review).

About the product

McAfee Drive Encryption is managed by McAfee's server-based ePolicy Orchestrator console (which can also be used to manage many other products). It allows full-disk encryption Windows Server/Windows client systems.

Product page on vendor's website

http://www.mcafee.com/hk/products/complete-data-protection.aspx

Good points

We found McAfee Drive Encryption to be straightforward to install and use. Although the manual lacks screenshots, it is comprehensive, and provides clear explanations. It is well laid-out and easy to navigate via bookmarks and a clickable contents page.

Tips for users

The *Menu* provides an at-a-glance overview of all the console's major features.

Documentation

Manuals

There is a comprehensive, 121-page guide to using the product available in .PDF format from the McAfee website.[5]

Knowledge base

There is a knowledge base on the McAfee website.[6]

[5] https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/24000/PD24867/en_US/de_710_product_guide_en_us_RevB.pdf

[6] https://support.mcafee.com/ServicePortal/faces/knowledgecenter?_adf.ctrl-state=1112me1q5h_70&p=Drive+Encryption&v=7.1.0&_afrLoop=825192279755000#!

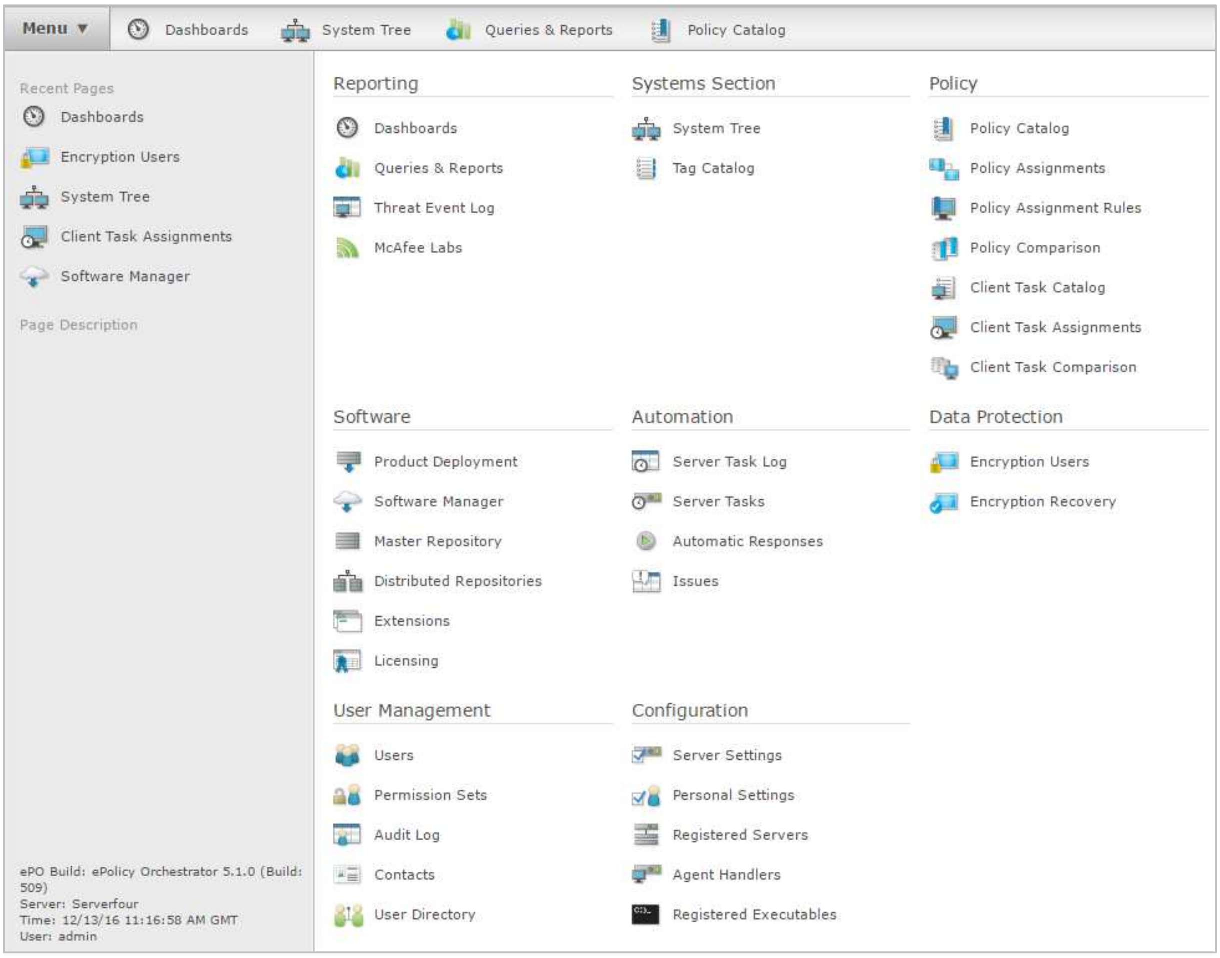
Management Console

Installation and configuration

To install the McAfee ePolicy Orchestrator console, the admin just needs to run the installer file and click through a straightforward setup wizard. Once the console is up and running and the admin has logged in, the Drive Encryption package has to be “checked in” to the console to allow it to be managed. This is a simple procedure and is described in the manual.

Layout

By default, ePolicy Orchestrator opens on the *Dashboards* page, which provides a graphical overview of managed systems using pie charts. Other pages are accessed from the toolbar at the top of the window, or the menu in the top left-hand corner:



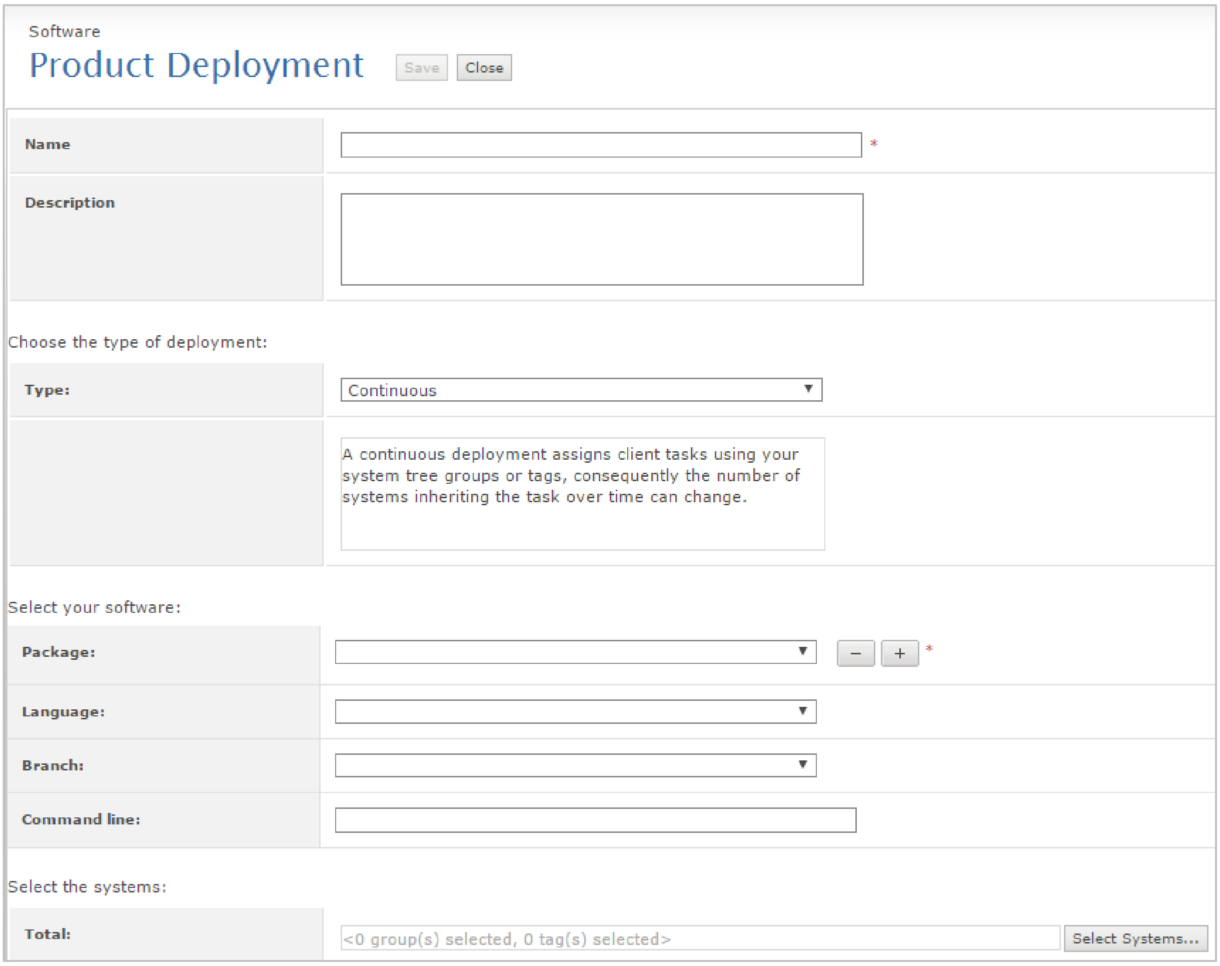
ePO Build: ePolicy Orchestrator 5.1.0 (Build: 509)
Server: Serverfour
Time: 12/13/16 11:16:58 AM GMT
User: admin

Preparing for deployment

Once the McAfee ePO agent has been installed on a client system, no further preparation is required before deployment can start.

Deploying the endpoint software

The endpoint encryption software is deployed via remote push installation. This can be done by clicking *Menu, Product Deployment, New Deployment*, and then entering details such as the product, language and systems to be installed in the *Product Deployment* task page:



Software

Product Deployment

Name	*
Description	

Choose the type of deployment:

Type:	Continuous
	A continuous deployment assigns client tasks using your system tree groups or tags, consequently the number of systems inheriting the task over time can change.

Select your software:

Package:	– + *
Language:	
Branch:	
Command line:	

Select the systems:

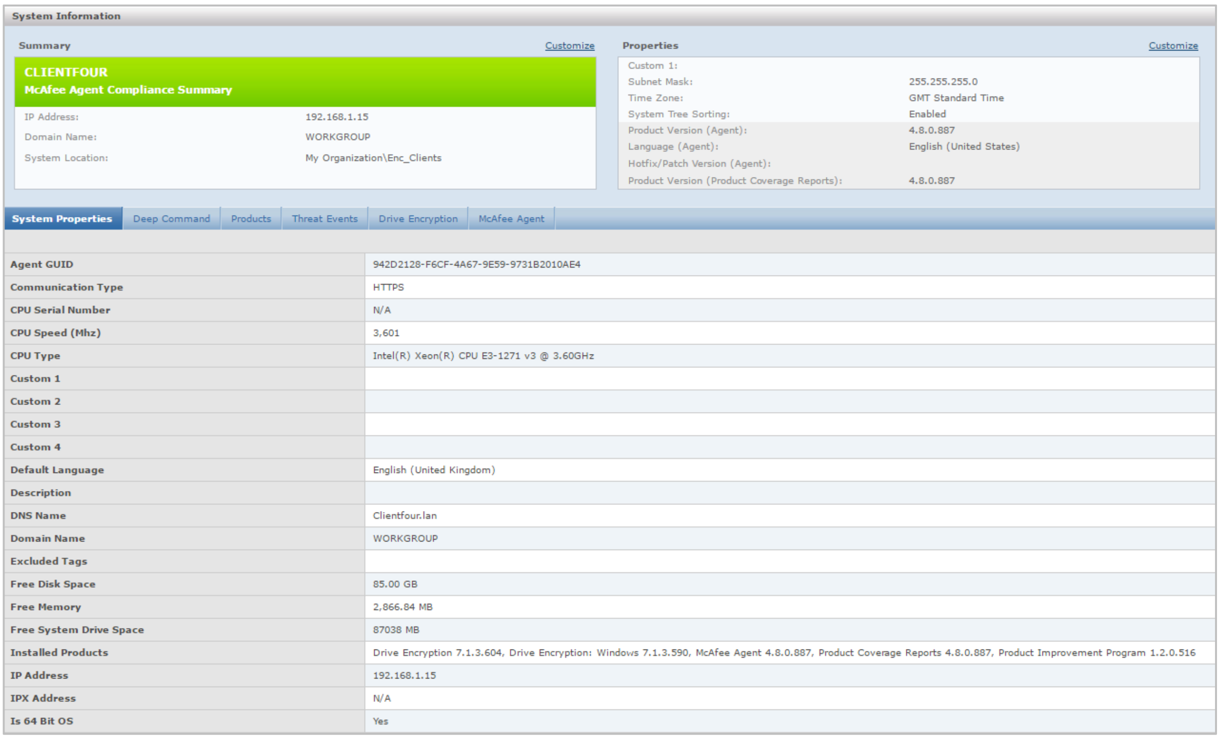
Total:	<0 group(s) selected, 0 tag(s) selected> Select Systems...

Systems to be installed should be restarted after the deployment task has been created, so that they pick up the new policy.

Monitoring the network

Workstations

The *Dashboard* page shows an overview of the network, listing e.g. installed PCs, version number and disk status. Clicking *System Tree*, then a specific group of workstations, shows a list of managed PCs in that group. The admin can click on an individual client PC to see a detailed properties page:



System Information

Summary

CLIENTFOUR
McAfee Agent Compliance Summary

IP Address:	192.168.1.15
Domain Name:	WORKGROUP
System Location:	My Organization\Enc_Clients

Properties

Custom 1:	
Subnet Mask:	255.255.255.0
Time Zone:	GMT Standard Time
System Tree Sorting:	Enabled
Product Version (Agent):	4.8.0.887
Language (Agent):	English (United States)
Hotfix/Patch Version (Agent):	
Product Version (Product Coverage Reports):	4.8.0.887

Agent GUID	942D2128-F6CF-4A67-9E59-9731B2010AE4
Communication Type	HTTPS
CPU Serial Number	N/A
CPU Speed (Mhz)	3,601
CPU Type	Intel(R) Xeon(R) CPU E3-1271 v3 @ 3.60GHz
Custom 1	
Custom 2	
Custom 3	
Custom 4	
Default Language	English (United Kingdom)
Description	
DNS Name	Clientfour.lan
Domain Name	WORKGROUP
Excluded Tags	
Free Disk Space	85.00 GB
Free Memory	2,866.84 MB
Free System Drive Space	87038 MB
Installed Products	Drive Encryption 7.1.3.604, Drive Encryption: Windows 7.1.3.590, McAfee Agent 4.8.0.887, Product Coverage Reports 4.8.0.887, Product Improvement Program 1.2.0.516
IP Address	192.168.1.15
IPX Address	N/A
Is 64 Bit OS	Yes

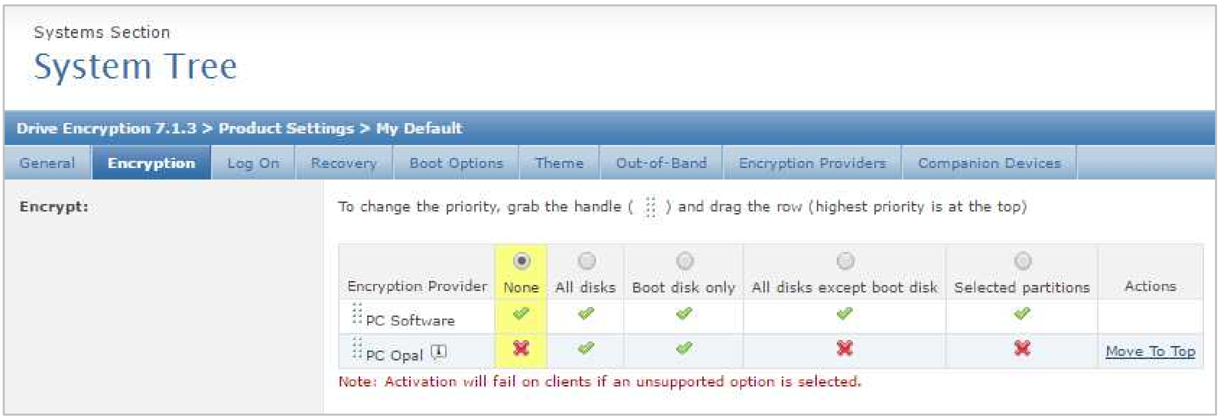
Users

Existing users can be managed, and new users added, by clicking *Menu, Users*.

Managing the network

Full disk encryption

Go to the relevant group in the System Tree, select a machine, click *Actions*, *Agent*, *Modify Policies on a Single System,* then *Product Settings, Edit Assignments* from the *Drive Encryption* product page. Here the admin can edit the existing policy, or apply a new one; in either case, the encryption settings of the policy can be configured to allow encryption of a specific disk or disks:



Systems Section

System Tree

Drive Encryption 7.1.3 > Product Settings > My Default

Encrypt:

To change the priority, grab the handle (⁞⁞) and drag the row (highest priority is at the top)

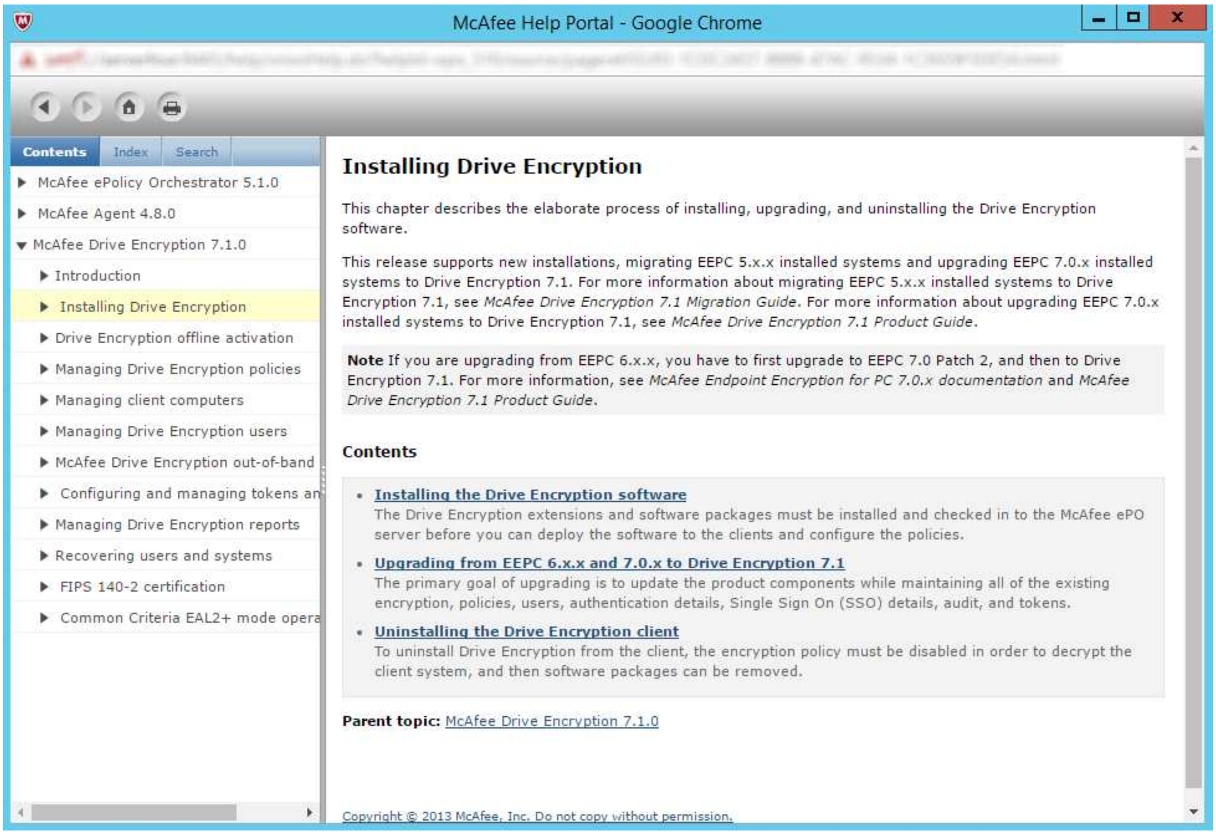
Encryption Provider	● None	○ All disks	○ Boot disk only	○ All disks except boot disk	○ Selected partitions	Actions
PC Software	✓	✓	✓	✓	✓	
PC Opal	✗	✓	✓	✗	✗	Move To Top

Note: Activation will fail on clients if an unsupported option is selected.

We selected *All Disks* in our test, and then saved the policy.

Integrated help feature

Clicking the *?* symbol in the top right-hand corner of the console window opens the local help service, which provides text instructions for Drive Encryption, plus the ePolicy Orchestrator console and its Agent:



- McAfee ePolicy Orchestrator 5.1.0
- McAfee Agent 4.8.0
- McAfee Drive Encryption 7.1.0
  - Introduction
  - Installing Drive Encryption
  - Drive Encryption offline activation
  - Managing Drive Encryption policies
  - Managing client computers
  - Managing Drive Encryption users
  - McAfee Drive Encryption out-of-band
  - Configuring and managing tokens an
  - Managing Drive Encryption reports
  - Recovering users and systems
  - FIPS 140-2 certification
  - Common Criteria EAL2+ mode opera

Installing Drive Encryption

This chapter describes the elaborate process of installing, upgrading, and uninstalling the Drive Encryption software.

This release supports new installations, migrating EEPC 5.x.x installed systems and upgrading EEPC 7.0.x installed systems to Drive Encryption 7.1. For more information about migrating EEPC 5.x.x installed systems to Drive Encryption 7.1, see *McAfee Drive Encryption 7.1 Migration Guide*. For more information about upgrading EEPC 7.0.x installed systems to Drive Encryption 7.1, see *McAfee Drive Encryption 7.1 Product Guide*.

Note If you are upgrading from EEPC 6.x.x, you have to first upgrade to EEPC 7.0 Patch 2, and then to Drive Encryption 7.1. For more information, see *McAfee Endpoint Encryption for PC 7.0.x documentation* and *McAfee Drive Encryption 7.1 Product Guide*.

Contents

- **Installing the Drive Encryption software**
  The Drive Encryption extensions and software packages must be installed and checked in to the McAfee ePO server before you can deploy the software to the clients and configure the policies.
- **Upgrading from EEPC 6.x.x and 7.0.x to Drive Encryption 7.1**
  The primary goal of upgrading is to update the product components while maintaining all of the existing encryption, policies, users, authentication details, Single Sign On (SSO) details, audit, and tokens.
- **Uninstalling the Drive Encryption client**
  To uninstall Drive Encryption from the client, the encryption policy must be disabled in order to decrypt the client system, and then software packages can be removed.

Parent topic: McAfee Drive Encryption 7.1.0

Copyright © 2013 McAfee, Inc. Do not copy without permission.

Windows client software

Installation

Installation of the Drive Encryption software on client PCs is carried out remotely from the console. The only thing to be installed on clients is the McAfee ePolicy Orchestrator Agent, which enables communication between client and server. This is done by creating an installation package in the console, which can be saved to a network share or USB drive, and then run on the client.

Program Interface

There is no user interface on the client PC; the product is managed entirely from the console. The McAfee Security Status message box, accessed from the McAfee Agent's System Tray icon, shows the status of the Drive Encryption Agent.

Email encryption

We could not find a means of encrypting emails with McAfee Drive Encryption.

Full disk encryption

This is managed from the console.

Removable media encryption

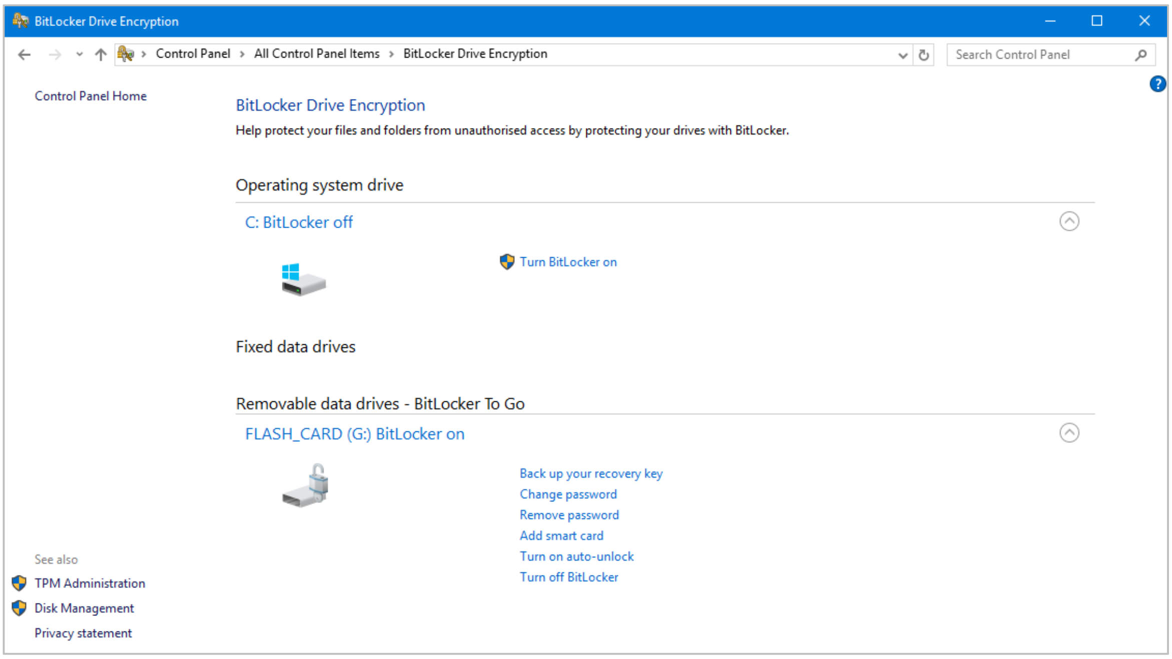
We could not find a means of encrypting removable media connected to the client PC via USB.

Recovery options for encrypted hard drives

User forgets password

If a user forgets their password for an encrypted system drive, they can click *Options, Recovery* at the password prompt, then select *Administrator/Smartphone Recovery*, which will display a challenge code. This is provided to the administrator. In the ePO console, the admin clicks *Menu, Data Protection, Encryption Recovery* and then enters the challenge code provided by the user. After clicking *Next*, the admin will see response codes which can be provided to the user to unlock the drive.

Microsoft BitLocker in Windows 10



BitLocker Drive Encryption

Help protect your files and folders from unauthorised access by protecting your drives with BitLocker.

Operating system drive

C: BitLocker off

Turn BitLocker on

Fixed data drives

Removable data drives - BitLocker To Go

FLASH_CARD (G:) BitLocker on

Back up your recovery key
Change password
Remove password
Add smart card
Turn on auto-unlock
Turn off BitLocker

Overview

Product version reviewed

For this review, we have looked at the BitLocker encryption features built into Windows 10 Enterprise, Version 1607 (Build 14393.447). The Pro and Education versions of Windows 10 include exactly the same interface and functionality.

Availability in other Windows operating systems

Windows Vista Ultimate and Enterprise Editions
Windows 7 Ultimate and Enterprise Editions
Windows 8/8.1 Pro and Enterprise Editions

Windows Server 2008/R2, 2012/R2, 2016

About the product

BitLocker encryption functionality is built into the Windows versions listed above. It allows users/admins to encrypt both complete system drives and removable media. It does not include any sort of central management feature, meaning that admins must encrypt individual devices locally, keep their own records of which devices have been encrypted, and arrange with individual users to keep backups of encryption keys etc.[7]

[7] Microsoft BitLocker Administration and Monitoring (MBAM) is a paid-for management console available to Microsoft business customers.

Product page on vendor's website

Not applicable

Good points

BitLocker offers easy-to-use basic encryption functionality for individual users with no installation or configuration required.

Tips for users

As there is no central management, system administrators should ensure that they distribute an encryption policy to all users, to ensure that there is a system for backing up everybody's recovery keys etc.

Documentation

Microsoft have various resources relating to BitLocker available online, such as this FAQ page: https://technet.microsoft.com/en-us/itpro/windows/keep-secure/bitlocker-frequently-asked-questions

Management Console

Not applicable

Windows client software

Installation

This is not applicable, as the feature is built into the operating system.

Program Interface

BitLocker on individual drives is accessed by right-clicking the drive and clicking the relevant BitLocker entry. The *BitLocker Drive Encryption* applet in Control Panel provides an overview of encrypted drives on the device, and management options for these (please see main screenshot at the beginning of this review).

Email encryption

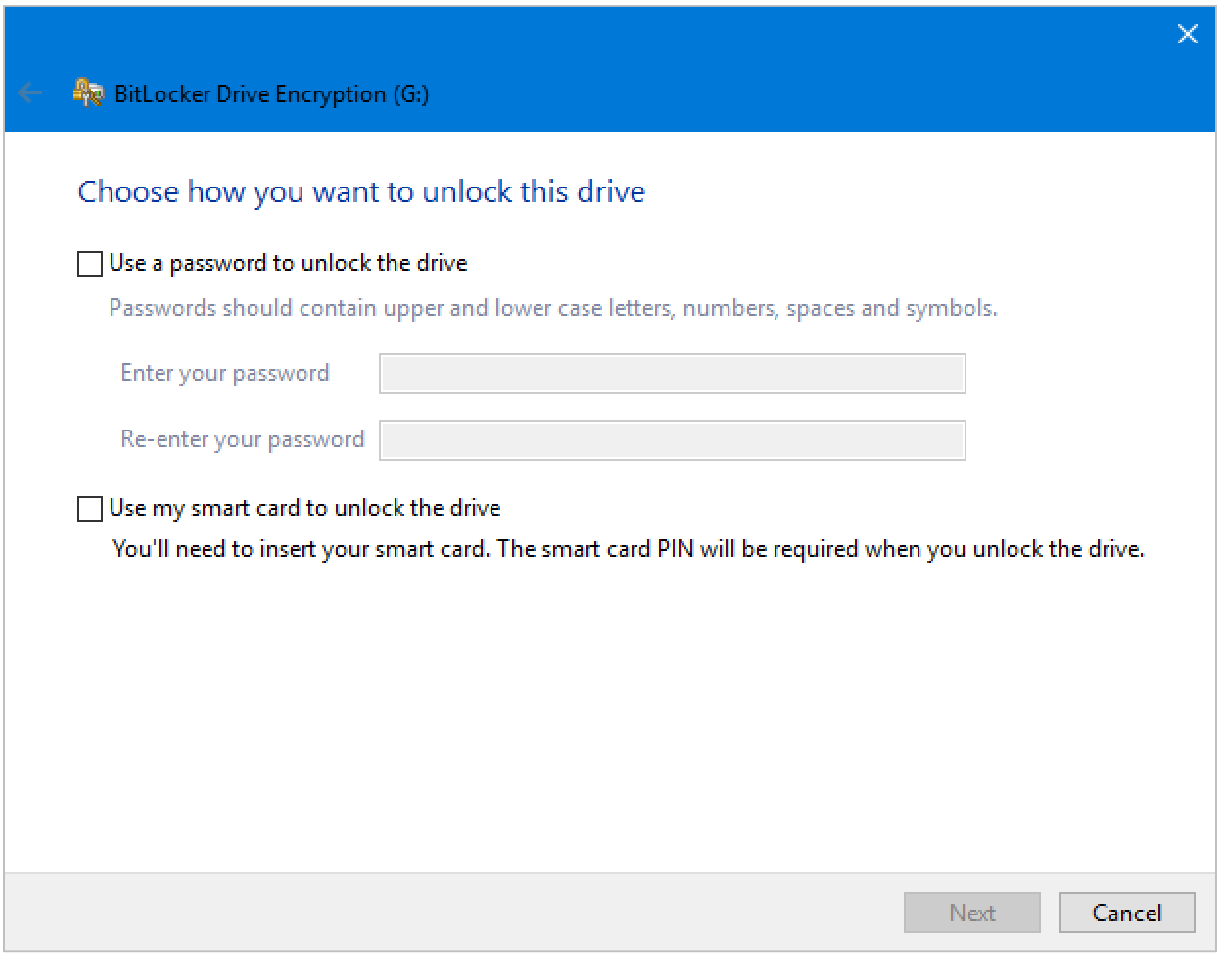
Not applicable

Full disk encryption

To encrypt an internal system drive, the user just right-clicks the drive in Windows Explorer, and then *Turn BitLocker on*. If the device does not have a Trusted Platform Module chip, the admin has to use the Group Policy Editor in Windows to allow the use of an alternative.[8]

Removable media encryption

To encrypt a removable drive, the user just right-clicks the drive in Windows Explorer, and then *Turn BitLocker on*. Windows then provides a choice of password or Smart Card to unlock the drive:



BitLocker Drive Encryption (G:)

Choose how you want to unlock this drive

□ Use a password to unlock the drive

Passwords should contain upper and lower case letters, numbers, spaces and symbols.

Enter your password

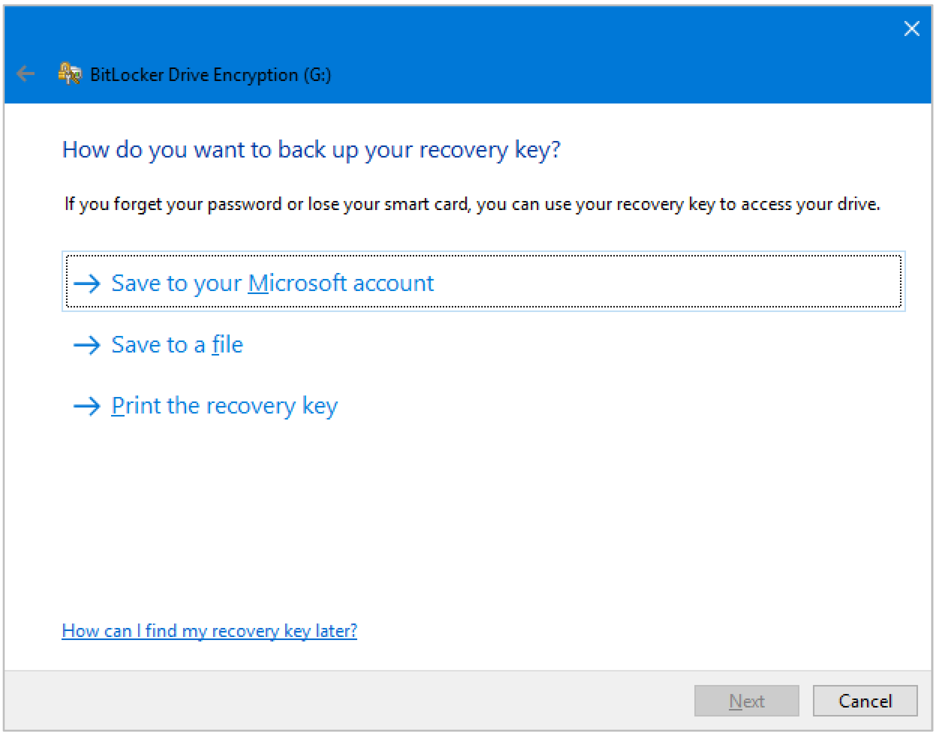
Re-enter your password

□ Use my smart card to unlock the drive

You'll need to insert your smart card. The smart card PIN will be required when you unlock the drive.

[8] https://answers.microsoft.com/en-us/windows/forum/windows_10/bitlocker-in-windows-10-without-tpm/f79add65-17c2-4a5d-92d6-e4d2a387119f

The next step is to save the recovery key, which will be needed to access the drive if the password or smart card is lost:



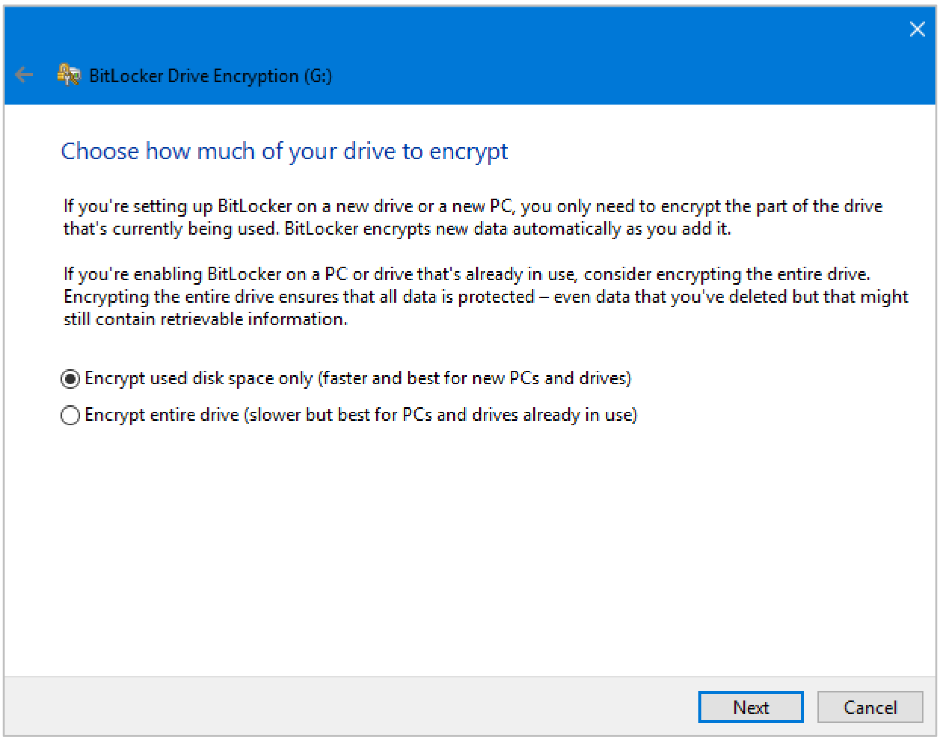
BitLocker Drive Encryption (G:)

How do you want to back up your recovery key?

If you forget your password or lose your smart card, you can use your recovery key to access your drive.

→ Save to your Microsoft account
→ Save to a file
→ Print the recovery key
How can I find my recovery key later?
Next
Cancel

The wizard then asks whether to encrypt the entire drive or only the used space:



Choose how much of your drive to encrypt

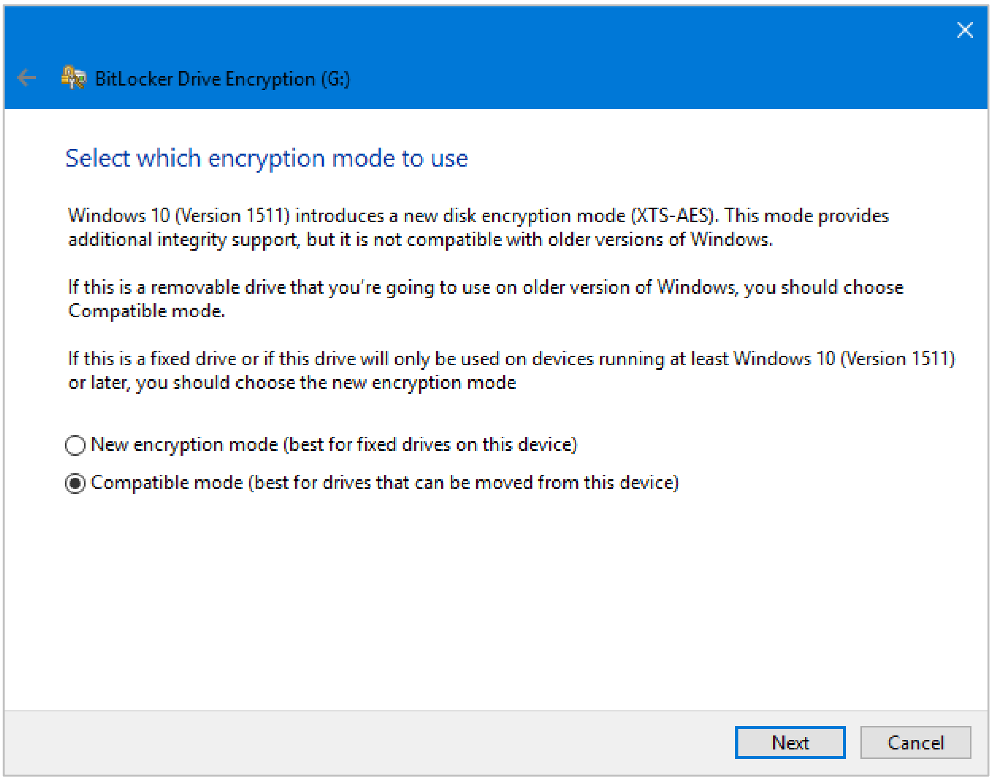
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.

If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected – even data that you've deleted but that might still contain retrievable information.

● Encrypt used disk space only (faster and best for new PCs and drives)

○ Encrypt entire drive (slower but best for PCs and drives already in use)

The next step is to decide whether to use the latest encryption mode, or a compatibility mode that will allow older versions of Windows to read the encrypted drive:



BitLocker Drive Encryption (G:)

Select which encryption mode to use

Windows 10 (Version 1511) introduces a new disk encryption mode (XTS-AES). This mode provides additional integrity support, but it is not compatible with older versions of Windows.

If this is a removable drive that you're going to use on older version of Windows, you should choose Compatible mode.

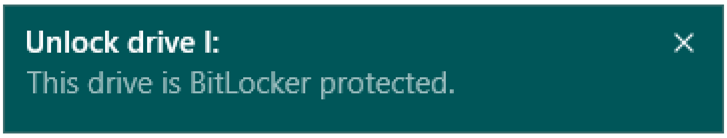
If this is a fixed drive or if this drive will only be used on devices running at least Windows 10 (Version 1511) or later, you should choose the new encryption mode

○ New encryption mode (best for fixed drives on this device)

● Compatible mode (best for drives that can be moved from this device)

After this, the user can start the encryption process (or cancel the operation).

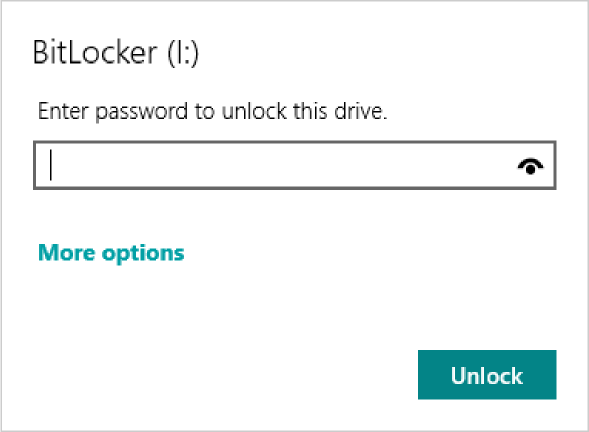
If the encrypted drive is then connected to any computer – including the one it was encrypted on – Windows will display a notification that the drive is protected by BitLocker:



Unlock drive I:

This drive is BitLocker protected.

Clicking this notification – or double-clicking the device in Windows Explorer – displays a password prompt to access the drive:



BitLocker (I:)

Enter password to unlock this drive.

Recovery options for encrypted hard drives

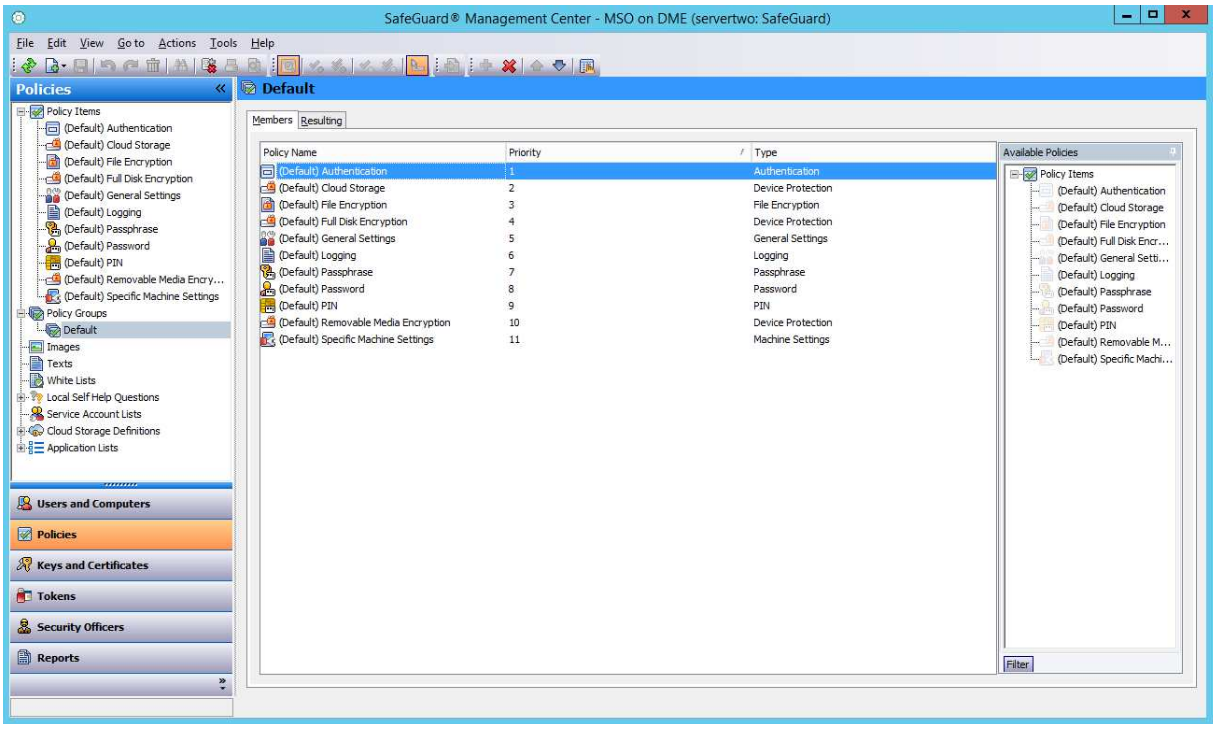
User forgets password

If the user forgets the password for an encrypted system drive, pressing the Esc key at the BitLocker password prompt allows the recovery key to be entered. Please note that this is only applicable to devices that do not have a Trusted Platform Module (TPM) chip.

Recovering data from the encrypted HDD of unbootable PC

Booting the system from a Windows PE bootable drive with the manage-bde.exe tool and recovery key allows data to be recovered from the encrypted system drive of an unbootable PC.

Sophos SafeGuard Enterprise



- Policy Items
  - (Default) Authentication
  - (Default) Cloud Storage
  - (Default) File Encryption
  - (Default) Full Disk Encryption
  - (Default) General Settings
  - (Default) Logging
  - (Default) Passphrase
  - (Default) Password
  - (Default) PIN
  - (Default) Removable Media Encry…
  - (Default) Specific Machine Settings
- Policy Groups
  - Default
- Images
- Texts
- White Lists
- Local Self Help Questions
- Service Account Lists
- Cloud Storage Definitions
- Application Lists

Policy Name	Priority	Type
(Default) Authentication	1	Authentication
(Default) Cloud Storage	2	Device Protection
(Default) File Encryption	3	File Encryption
(Default) Full Disk Encryption	4	Device Protection
(Default) General Settings	5	General Settings
(Default) Logging	6	Logging
(Default) Passphrase	7	Passphrase
(Default) Password	8	Password
(Default) PIN	9	PIN
(Default) Removable Media Encryption	10	Device Protection
(Default) Specific Machine Settings	11	Machine Settings

- Policy Items
  - (Default) Authentication
  - (Default) Cloud Storage
  - (Default) File Encryption
  - (Default) Full Disk Encr…
  - (Default) General Setti…
  - (Default) Logging
  - (Default) Passphrase
  - (Default) Password
  - (Default) PIN
  - (Default) Removable M…
  - (Default) Specific Machi…

Overview

Product version reviewed

SafeGuard Management Center 8.00.2.13

Sophos SafeGuard client software 8.00.0.251

Windows operating systems supported

Management Center: Windows 7, 8.1, 10; Windows Server 2008/R2, 2012/R2

Client encryption software: Windows XP, Vista, 7, 8.1, 10

Server encryption software: Windows Server Windows Server 2008/R2, 2012/R2

The SafeGuard Enterprise Server component has to be installed on a Windows Server operating system, though an Active Directory domain is not required.

Other supported platforms

Sophos SafeGuard is also supported on Apple OS X and Android devices (not covered in this review).

About the product

Sophos SafeGuard allows the encryption of complete system drives, removable media and individual files, and is managed centrally from a server-based console.

Product page on vendor's website

https://www.sophos.com/en-us/products/safeguard-encryption.aspx

Good points

The management console is easy for admins to navigate due to its similarity to the .MMC consoles found in Windows. The *Local Self Help* method of password recovery enables a user to recover a lost password without having to contact the administrator.

Tips for users

Experience of Microsoft SQL Server and Internet Information Services is valuable when installing the console. Experienced system administrators who are used to e.g. corporate antivirus software will find the policy-based encryption methods familiar.

Documentation

Manuals

A range of manuals is available:

https://www.sophos.com/en-us/support/documentation/safeguard-enterprise.aspx#

Knowledge base

A searchable online knowledge base is provided:

https://community.sophos.com/kb?TopicId=1371

Management Console

Installation and configuration

Sophos SafeGuard requires additional software to be set up on the server before the product itself is installed; these items are listed under *Prerequisites* in the online manual, and include Microsoft Internet Information Services, .NET Framework 4.5 and ASP.NET 4.5, Universal C Runtime and Microsoft SQL Server.

Two Sophos components, SafeGuard Enterprise Server and SafeGuard Management Center, can then be installed by completing two straightforward setup wizards.

Layout

The SafeGuard management console uses a similar layout to the Microsoft Management Console, with a tree of items in a narrow left-hand pane, and a main right-hand pane to display details and options of the currently selected item.

Preparing for deployment

Under *Prepare endpoint computers for encryption,* the manual lists steps to be taken on client PCs before installing the encryption software. These include some general maintenance items, such as checking for disk space and running chkdsk.exe, and running the Sophos pre-installation package.

Deploying the endpoint software

The client encryption software can be deployed by push installation or running the setup file locally on the client. We used the latter method for our test. The installer file is created from the console, by running the Configuration Package Tool and saving the .MSI created to a network share/USB flash drive.

Monitoring the network

Workstations

These can be managed by clicking the *Users and Computers* button in the bottom left-hand corner of the console window.

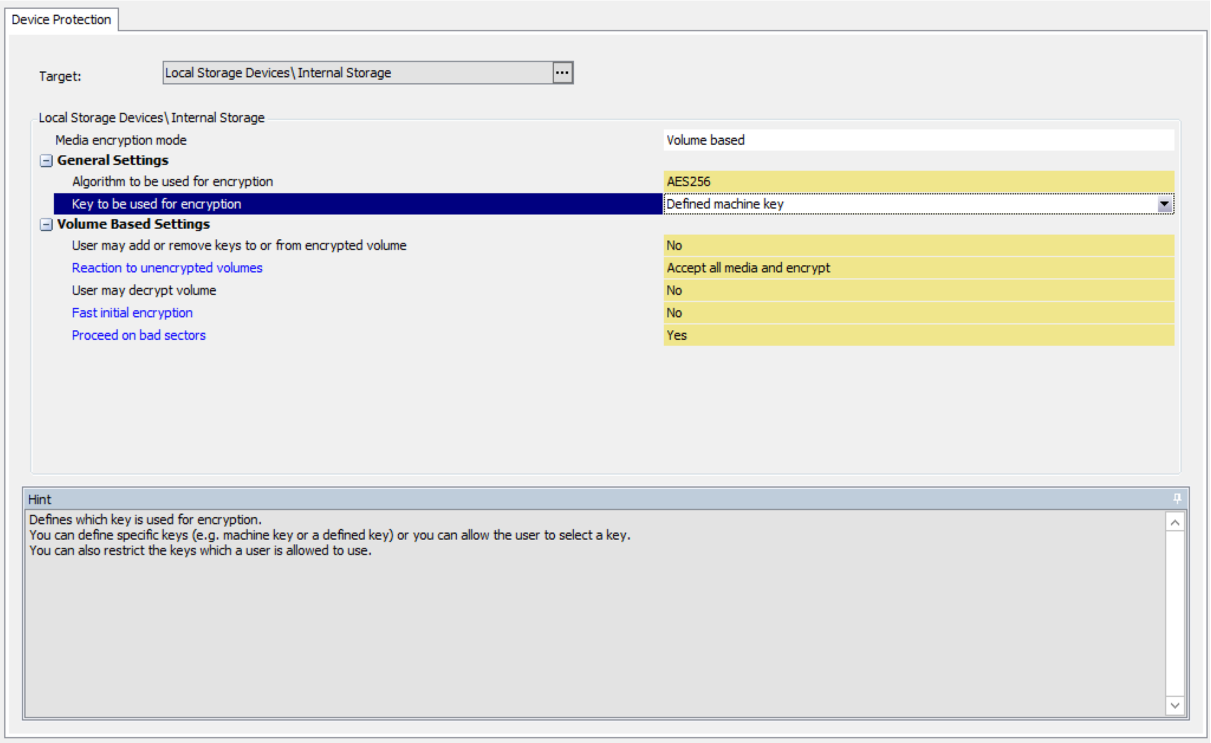
Users

These can be managed by clicking the *Users and Computers* button in the bottom left-hand corner of the console window.

Managing the network

Full disk encryption

This is carried out by creating/editing a policy under *Policies*, and assigning it to the appropriate devices.



Target: Local Storage Devices\Internal Storage

Local Storage Devices\Internal Storage

Media encryption mode	Volume based
General Settings	
Algorithm to be used for encryption	AES256
Key to be used for encryption	Defined machine key
Volume Based Settings	
User may add or remove keys to or from encrypted volume	No
Reaction to unencrypted volumes	Accept all media and encrypt
User may decrypt volume	No
Fast initial encryption	No
Proceed on bad sectors	Yes

Hint

Defines which key is used for encryption.
You can define specific keys (e.g. machine key or a defined key) or you can allow the user to select a key.
You can also restrict the keys which a user is allowed to use.

Integrated help feature

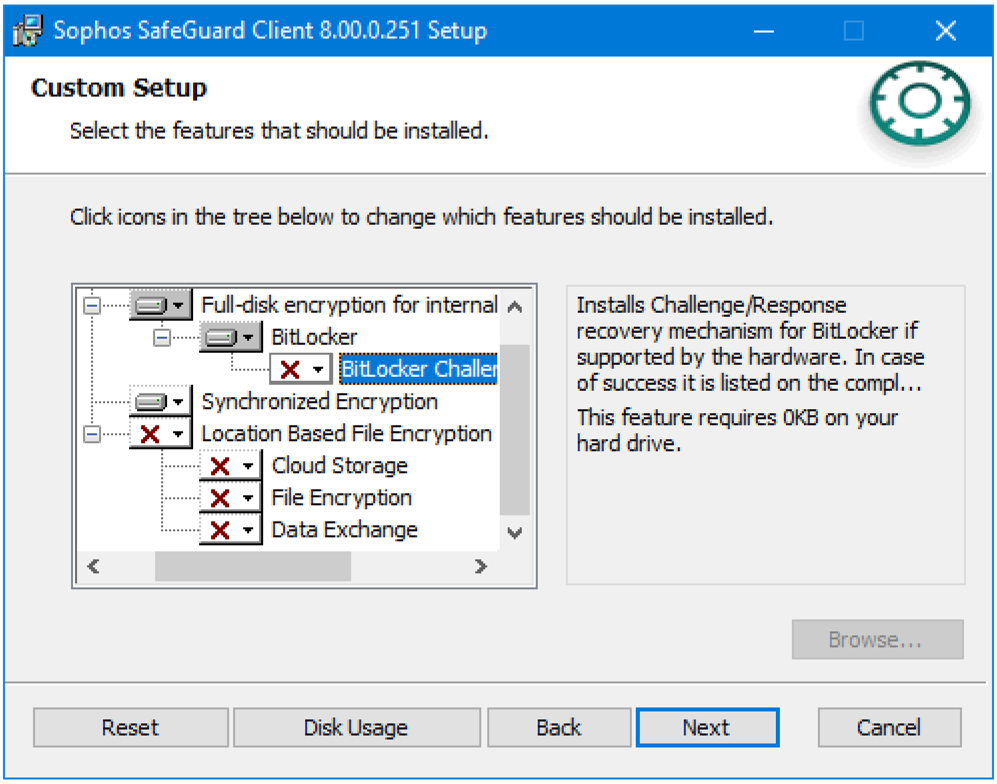
Clicking *Help, Help topics* in the console window opens the program's online help pages:

https://docs.sophos.com/esg/sgn/8-0/admin/win/en-us/webhelp/index.htm#concepts/Welcome.htm

Windows client software

Installation

To install the software on a client, the admin needs to download a configuration file called POACFG from the Sophos website, and then run the installer from a command prompt command that includes both the .MSI installer and configuration files. The setup wizard requires the admin to accept the EULA; optionally, it is possible to change the installation folder and select features:



Sophos SafeGuard Client 8.00.0.251 Setup

Custom Setup

Select the features that should be installed.

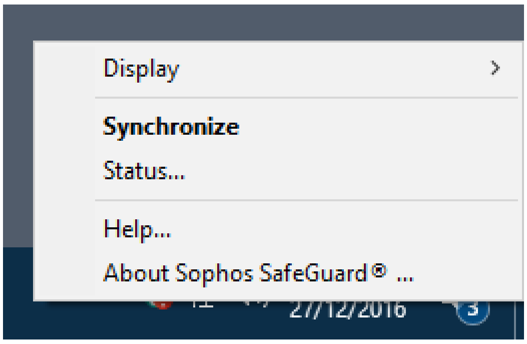
Click icons in the tree below to change which features should be installed.

Installs Challenge/Response recovery mechanism for BitLocker if supported by the hardware. In case of success it is listed on the compl…

This feature requires 0KB on your hard drive.

Program Interface

The SafeGuard System Tray icon displays a menu when right-clicked, although this is oriented towards system administrators rather than end users:



Email encryption

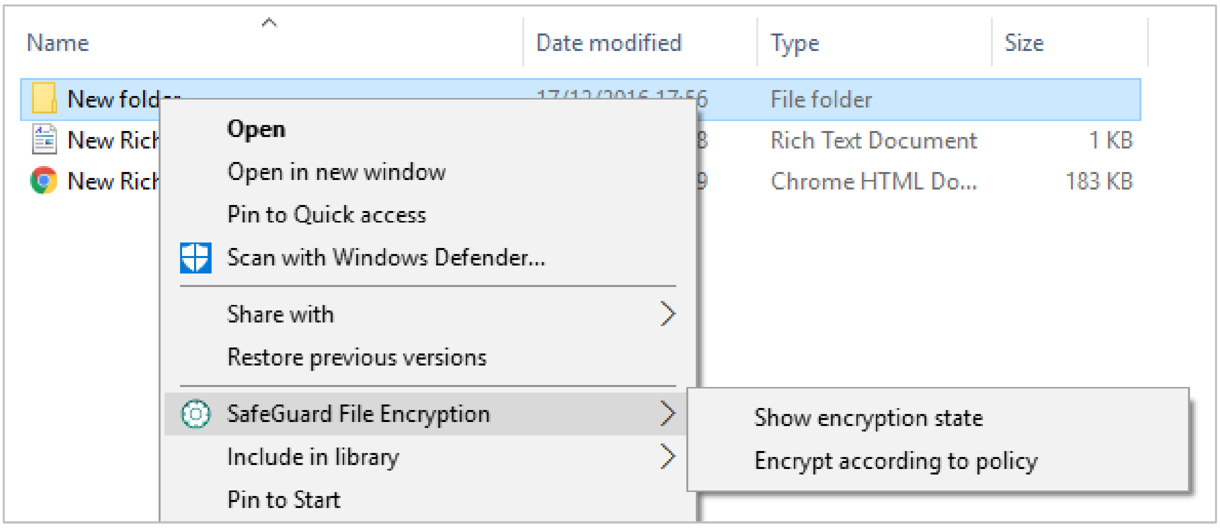
We could not find a means of encrypting emails using Sophos SafeGuard.

Full disk encryption

This is managed from the console.

File and folder encryption

Individual files and folders can be encrypted by right-clicking the file or folder, and selecting *Encrypt according to policy* in the SafeGuard sub-menu:



For files, there is an additional option, *Create password protected file*.

Removable media encryption

This can be encrypted in the same way as for files and folders, described above.

Recovery options for encrypted hard drives

User forgets password

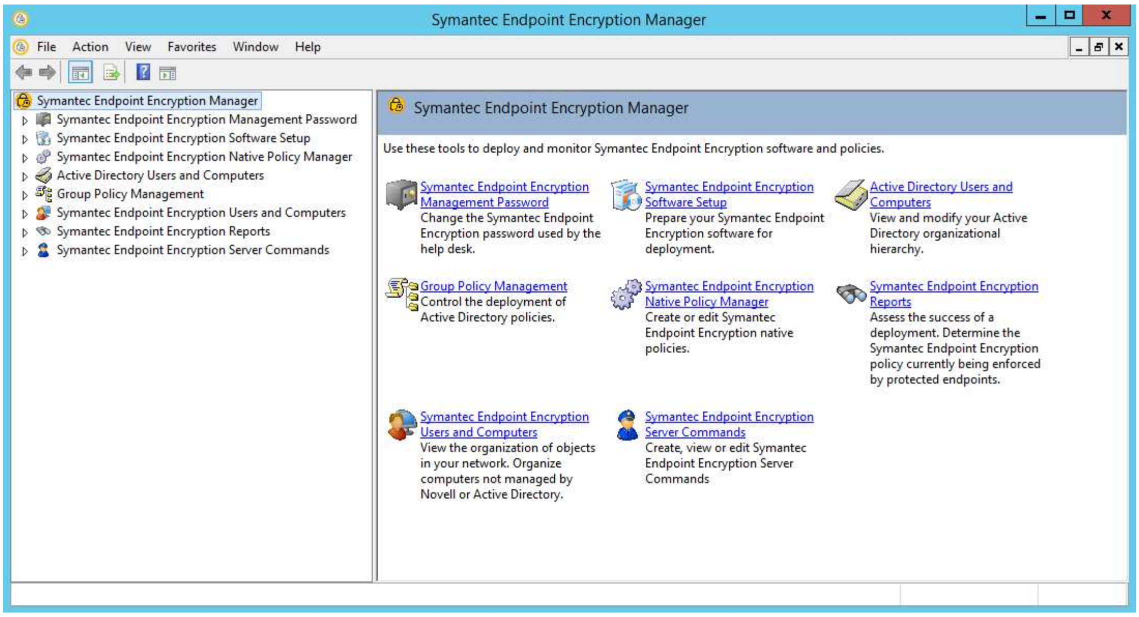
There are two methods of recovering a forgotten password, namely *Local Self Help* and *Challenge/Response*. Sophos recommends the *Local Self Help* option, which involves the user entering their username at the logon screen and clicking *Recover*, then *Local Self Help* if both options are displayed. The system then asks the user a number of predefined and pre-recorded questions stored on the local computer. If the user answers these successfully, the password is displayed for a few seconds.

Recovering data from the encrypted HDD of unbootable PC

Data can be recovered from the encrypted system drive of an unbootable PC using a WinPE environment, available to download as an .ISO file from the Sophos website:

https://community.sophos.com/kb/en-us/108805

Symantec Endpoint Encryption


Symantec Endpoint Encryption Manager
File
Action
View
Favorites
Window
Help
Symantec Endpoint Encryption Manager
Symantec Endpoint Encryption Management Password
Symantec Endpoint Encryption Software Setup
Symantec Endpoint Encryption Native Policy Manager
Active Directory Users and Computers
Group Policy Management
Symantec Endpoint Encryption Users and Computers
Symantec Endpoint Encryption Reports
Symantec Endpoint Encryption Server Commands

Symantec Endpoint Encryption Manager

Use these tools to deploy and monitor Symantec Endpoint Encryption software and policies.

Symantec Endpoint Encryption Management Password
Change the Symantec Endpoint Encryption password used by the help desk.

Symantec Endpoint Encryption Software Setup
Prepare your Symantec Endpoint Encryption software for deployment.

Active Directory Users and Computers
View and modify your Active Directory organizational hierarchy.

Group Policy Management
Control the deployment of Active Directory policies.

Symantec Endpoint Encryption Native Policy Manager
Create or edit Symantec Endpoint Encryption native policies.

Symantec Endpoint Encryption Reports
Assess the success of a deployment. Determine the Symantec Endpoint Encryption policy currently being enforced by protected endpoints.

Symantec Endpoint Encryption Users and Computers
View the organization of objects in your network. Organize computers not managed by Novell or Active Directory.

Symantec Endpoint Encryption Server Commands
Create, view or edit Symantec Endpoint Encryption Server Commands

Overview

Product version reviewed

Symantec Endpoint Encryption 11.1.0

Windows operating systems supported

Management server: Windows Server 2008, 2012

Management console and client: Windows Server 2008, 2012; Windows 7, 8, 8.1, 10

The Symantec Endpoint Encryption server has to be installed on a Windows Server operating system that is a member of an Active Directory domain.

Other supported platforms

Mac OS X

About the product

Symantec Endpoint Encryption uses a server-based console to manage encryption of Windows client and server operating systems.

Product page on vendor's website

https://www.symantec.com/products/information-protection/encryption/endpoint-encryption

Good points

The Symantec Endpoint Encryption Manager uses Microsoft's MMC console, which will be familiar and easy to navigate for all Windows system administrators. This displays the Active Directory structure of the network, making it very straightforward to find computers/groups in the pre-existing structure. Once the client software has been installed, starting disk encryption can be done with a couple of clicks. There is a range of options for removable media encryption.

Tips for users

We would recommend admins to read the details of the software prerequisites in the *Installation Guide* before proceeding with installation. Experience of Microsoft SQL Server and Internet Information Services is very helpful.

Documentation

Manuals

A wide range of documentation is available on the Symantec support website.[9]

Knowledge base

An online knowledge base is provided.[10]

Management Console

Installation and configuration

Symantec Endpoint Encryption consists of two major components, the server (backend) and management console (user interface). The server component has to be installed on a Windows Server OS, and requires additional Microsoft software to be installed first, namely Internet Information Services (IIS), .NET 3.5 and 4.5, and SQL Server. Precise details of the components to be installed can be found in the *Installation Guide*. Once these prerequisites have been met, the management server can be installed using a straightforward setup wizard. The management console can be installed on the same computer as the backend, and/or other servers or workstation, again using a simple installation wizard.

Layout

Symantec Endpoint Encryption Manager uses the Microsoft MMC console, which will be familiar to all Windows administrators. The main configuration items are listed in the console tree in the left-hand pane; clicking on one of these displays the details in the larger right-hand pane.

[9] https://support.symantec.com/en_US/endpoint-encryption.html
[10] https://support.symantec.com/en_US/endpoint-encryption.html

Preparing for deployment

Before deploying the software, we enabled file sharing and network discovery on client PCs.

Deploying the endpoint software

This can be done by creating an installation package under *Symantec Endpoint Encryption Software Setup, Windows Client*, and saving the installer to a network share, from where it can be run on client PCs.

Monitoring the network

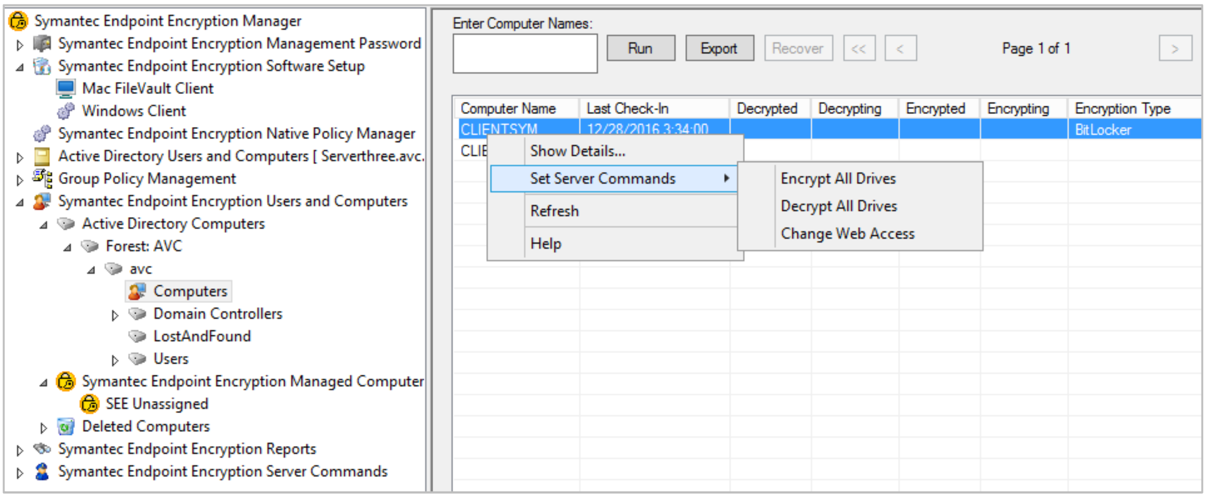
Workstations and Users

These can be seen under *Symantec Endpoint Encryption Users and Computers*, then the appropriate Active Directory Forest/domain/GPO.

Managing the network

Full disk encryption

Disk encryption can be started very simply by locating the PC to be encrypted in *Symantec Endpoint Encryption Users and Computers*, then right-clicking it, pointing to Set *Server Commands* and clicking *Encrypt All Drives*.


Symantec Endpoint Encryption Manager
Symantec Endpoint Encryption Management Password
Symantec Endpoint Encryption Software Setup
Mac FileVault Client
Windows Client
Symantec Endpoint Encryption Native Policy Manager
Active Directory Users and Computers [Serverthree.avc.
Group Policy Management
Symantec Endpoint Encryption Users and Computers
Active Directory Computers
Forest: AVC
avc
Computers
Domain Controllers
LostAndFound
Users
Symantec Endpoint Encryption Managed Computer
SEE Unassigned
Deleted Computers
Symantec Endpoint Encryption Reports
Symantec Endpoint Encryption Server Commands
Enter Computer Names:
Run
Export
Recover
<<
<
Page 1 of 1
>
Show Details...
Set Server Commands
Refresh
Help
Encrypt All Drives
Decrypt All Drives
Change Web Access

Computer Name	Last Check-In	Decrypted	Decrypting	Encrypted	Encrypting	Encryption Type
CLIENTSYM	12/28/2016 3:34:00					BitLocker
CLIE						

Integrated help feature

We could not find an integrated help feature in the console.

Windows client software

Installation

This involves running the installer package created with the console (as described above). There are no choices to be made, and setup completes very quickly with no further input required.

Email encryption

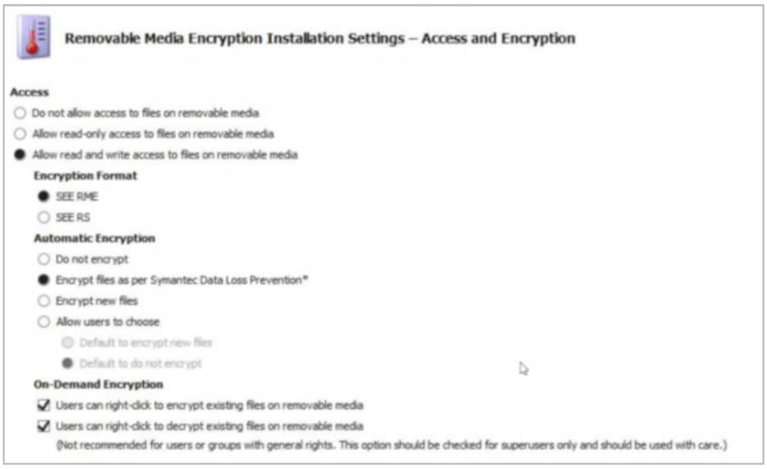
This is not included in the product.

Full disk encryption

This is carried out from the console, as described above.

Removable media encryption

Options for this are set in the console, and the user experience will vary according to these settings. The admin can choose to block removable media completely, allow read-only access, encrypt devices automatically, encrypt new files automatically, or allow the user to choose what to do:



Removable Media Encryption Installation Settings – Access and Encryption

Access
○ Do not allow access to files on removable media
○ Allow read-only access to files on removable media
● Allow read and write access to files on removable media

Encryption Format
● SEE RME
○ SEE RS

Automatic Encryption
○ Do not encrypt
● Encrypt files as per Symantec Data Loss Prevention*
○ Encrypt new files
○ Allow users to choose
○ Default to encrypt new files
● Default to do not encrypt

On-Demand Encryption
☑ Users can right-click to encrypt existing files on removable media
☑ Users can right-click to decrypt existing files on removable media
(Not recommended for users or groups with general rights. This option should be checked for superusers only and should be used with care.)

Recovery options for encrypted hard drives

User forgets password

There are two methods of gaining access to a PC if the user has forgotten their password. Firstly, the user can press the F4 key on the keyboard, which will display preconfigured security questions for the user to answer. If these are answered correctly, the user will be able to access the PC and change their password.

Recovering data from the encrypted HDD of unbootable PC

ISO files to create bootable recovery devices are available on the Symantec website.

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 (January 2017)