

DESlock+ UEFI Release

Changes to DESlock+ Enterprise Server and Client to support UEFI

Version	1.4
Date	19 th November 2014
Status	See change history



Table of Contents

Purpose.....	3
Change History	3
Applies To	3
Full Disk Encryption	4
UEFI, GPT & Windows 8.....	4
Improved Compatibility Checks.....	4
Safe Start mode	5
Multiple Partitions, Multiple Disks	6
Hardware RAID & Intel Rapid Storage Technology	6
Enterprise Server User Interface	6
Unmanaged User Interface	7
Enterprise Server	8
New Look	8
Licensing	8
Emails.....	9
Active Directory Synchronisation	9
Secure Webserver Configuration (SSL/HTTPS).....	10
SMTP Support for Gmail / TLS	10
Workstation Information Logs.....	11
User Activation	12
DESlock+ Mobile	12



Purpose

The purpose of this document is to detail the changes that have been made in the latest (September 2014) DESlock+ Enterprise Server and Client. The document describes the most significant changes, where either new functionality has been added or the user experience has changed.

Change History

VERSION	DATE	AUTHOR	DESCRIPTION
1.0	22 nd September 2014	Duncan Hume	Initial document
1.1	26 th September 2014	Duncan Hume	Added Unmanaged Full Disk Encryption UI
1.2	30 th September 2014	Duncan Hume	Updated email template details
1.3	6 th October 2014	Duncan Hume	Added Applies to Section
1.4	19 th November 2014	Duncan Hume	Added full release to Applies to Section

Applies To

This document applies to the following versions of DESlock+

Description	DATE	VERSION
Release Candidate 1	22 nd September 2014	DESlock+ Client 4.6.9
		Enterprise Server 2.4.23
Release Candidate 2	1 st October 2014	DESlock+ Client 4.6.14
		Enterprise Server 2.5.0
Full Release	18 th November 2014	DESlock+ Client 4.7.4+
		Enterprise Server 2.5.2+



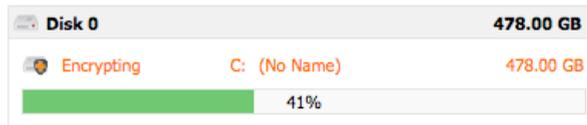
Full Disk Encryption

UEFI, GPT & Windows 8

The main purpose of this release is to provide support for Full Disk Encryption on Windows 8 with UEFI. New systems that ship with Windows 8 (or 8.1 etc.) may be configured in UEFI mode. This release allows these systems to be Full Disk Encrypted by adding UEFI and GPT disk support.

Hardware Information

Manufacturer: Dell Inc.
Model: OptiPlex 9020
Boot Mode: UEFI
BIOS Version: A05



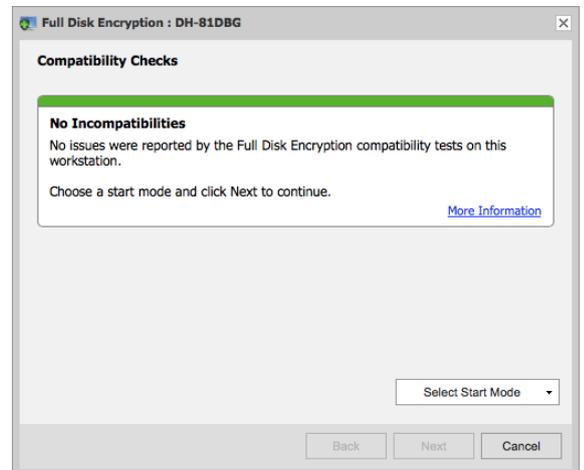
Full Disk Encryption with UEFI systems is not specific to Windows 8; Windows 7 x64 is also supported.

Improved Compatibility Checks

In previous versions, the DESlock+ client carried out compatibility checks when the command to start Full Disk Encryption was received. Attempting to start Full Disk Encryption on a system that may not be compatible could result in an error being returned to the Enterprise Server. In some cases the compatibility checks could be overridden and Full Disk Encryption would succeed. However in some cases, this would result in the system becoming unbootable, with the only course of action being to use the DESlock+ Recovery CD.

With the new release, the DESlock+ Client reports compatibility information to the Enterprise Server before Full Disk Encryption is started. This enables the Enterprise Server to display information about compatibility and allow the encryption to proceed or not, without having to send the command to the workstation.

Results of the compatibility checks are listed in the Enterprise Server at the beginning of the Full Disk Encryption wizard. This includes any incompatible software found, disks already encrypted with other software, warnings and suggestions for how to proceed.

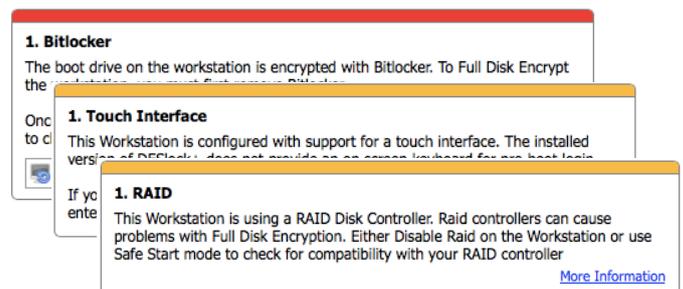


There are 3 types of compatibility items, each shown in a different colour.

Green items contain information about the system.

Yellow items contain warnings, including any special conditions or actions to perform to successfully start encryption.

Red items contain incompatibilities. These include any issues found that will prevent encryption from working.



A start mode must be selected to start Full Disk Encryption from the Enterprise Server. Which start mode is available depends on the results of the compatibility checks. In normal operation either Normal mode or Safe Start mode are available. If any warning items (Yellow) are reported, then only Safe Start will be available. If any incompatibilities (Red) are reported then encryption cannot be started.

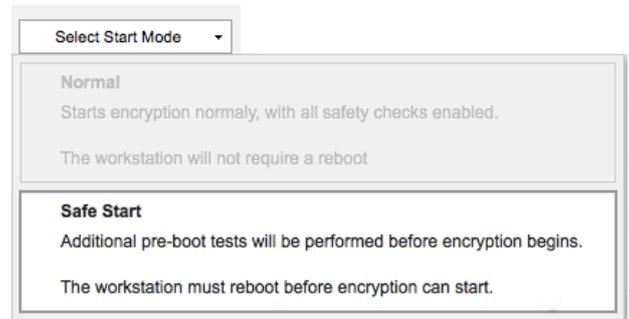
Normal Start mode starts encryption in the same way as previous version of DESlock+. This follows password & user options set in the wizard. This option does not require a reboot.

Safe Start mode introduces new functionality to test for Full Disk Encryption compatibility, see the next section for details.

Safe Start mode

This release introduces Safe Start mode, which provides a means to test for system compatibility with Full Disk Encryption.

Safe Start mode is the recommended way to start Full Disk Encryption, in some circumstances; Safe Start mode will be the only option available. This depends on any compatibility issues that may have been found.



Safe-Start Mode changes the current FDE process by postponing encryption until the DESlock+ boot loader has successfully run. During Safe Start mode the system must be rebooted.

To begin, DESlock+ installs the boot loader then restarts the system. In Safe Start mode, the boot loader does not require user credentials to be entered and, after a short delay, continues to boot the system.

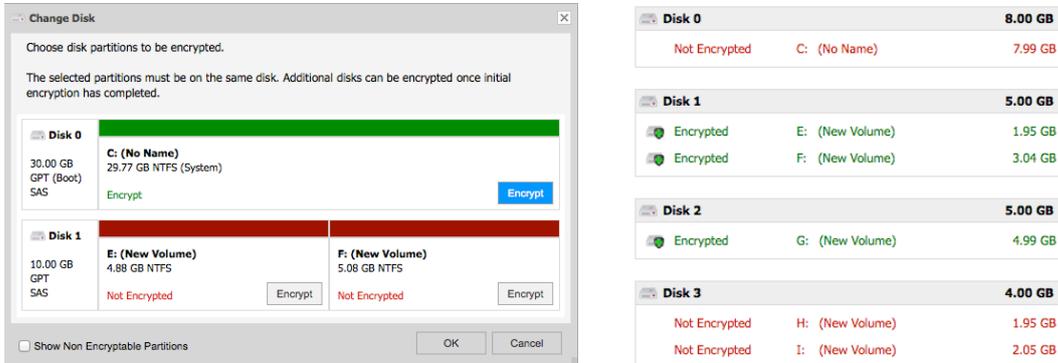
If the resident portion of the DESlock+ boot loader is detected, the FDE process continues. The user is asked for their credentials and encryption starts.

If the DESlock+ boot loader does not run successfully and the system does not boot, the original system state is restored. The system will then restart as normal, with no recovery required.



Multiple Partitions, Multiple Disks

Full Disk Encryption has been further improved by providing support through the Enterprise Server for selecting disks & partitions to be encrypted.



When starting full disk encryption, partitions on the main system disk are automatically selected. Partitions on other disks can be selected, but only one disk can be operated one at a time. Partitions that cannot be encrypted are not displayed; they can be viewed using the 'Show Non Encryptable Partitions' option. Once encryption is complete further disks can be encrypted. Individual partitions can also be decrypted using the same interface.

Hardware RAID & Intel Rapid Storage Technology

This release provides updated support for systems with RAID controllers, Intel RST and 'RAID Ready'. This includes systems from well known manufacturers such as DELL, HP and IBM that are pre-configured with a single disk in RAID mode.

Earlier versions of DESlock could cause problems with some of these systems. With the addition of a revised boot loader and the introduction of Safe Start mode, use on unsupported hardware should not result in an un-bootable system.

Enterprise Server User Interface

In the Enterprise Server, Full Disk Encryption can now be started directly from the workstation details, or as before from the user window.

Starting Full Disk Encryption now consists of a wizard that leads you through the settings. This includes the compatibility checks, user login information and disk partition selection.

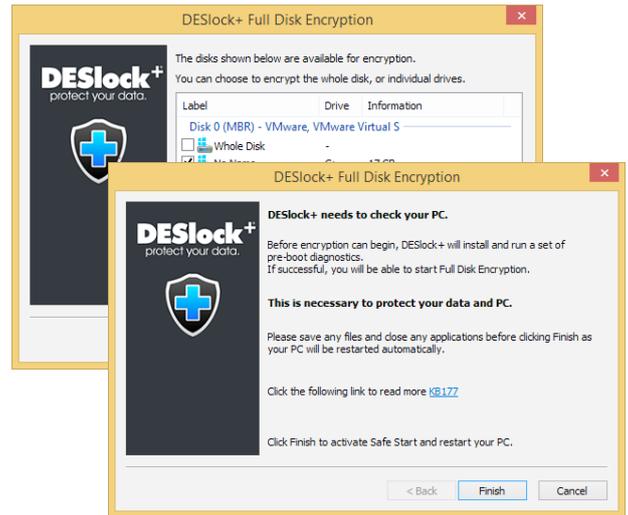
The Enterprise Server interface for adding a new Full Disk Encryption login has also been improved, making adding additional users to a workstation easier.



Unmanaged User Interface

The unmanaged (standalone) client user interface for starting Full Disk Encryption has also been improved.

Starting encryption when unmanaged now always uses Safe Start mode. This performs the same function as with managed mode and requires a restart before encryption will begin. (See Safe Start section)



When starting Full Disk Encryption DESlock+ automatically generates an admin login and password. This login and password is required to make any changes to encryption, to modify user logins or if a user password is forgotten. It is important that admin login credentials be kept safe.

Unmanaged Full Disk Encryption requires that the admin credentials be saved before encryption can be started. The credentials are now saved to an html file that contains more detailed information.



Enterprise Server

New Look

The look and feel of the Enterprise Server interface has changed, giving it a more flat look. However, the basic structure of the interface has not changed.



Users
Stores users within the Enterprise Server.
Once users are activated on a workstation, policy can be applied to them via the Group Policy panel.

Users 15 | Teams | Encryption Key Groups | Keys | Group Policy | Updates | Alerts

Details | Add | Edit | Move | Delete | Generate Activation Codes | Post Key-File | All Users

Email	Name	Full Name	Status
-------	------	-----------	--------

Licensing

Previous versions of the Enterprise Server supported multiple licence types, however only one licence could be applied to a user. This update adds the ability to licence users with more than one product type.

There are currently two product types available.

- Windows – The DESlock+ Windows Client, which includes the normal licence types: Pro, Standard Edition and Essential Edition.
- Mobile – Currently DESlock+ Mobile is available for iOS devices.

Licence Details

Active Licence(s):	Licence Type	Serial Number	Expiry Info
	Mobile	800039C7	Support expires Tue, Nov 11 2014
	Standard Edition Trial	800039C8	Trial expires Sat, Dec 13 2014

A user can now be licensed for each product type but only with 1 type of licence from each product type e.g.

*DESlock+ Pro and DESlock+ Mobile or
DESlock+ Essential Edition or
DESlock+ Mobile*

A user is automatically licensed when an activation code is generated. To support the new licensing, the activation interface has also changed.

When generating activation codes, the product type for the licence must first be selected *. Then if the user is not already licensed, a specific multi user licence can be chosen for that product type.

Generate Activation Codes

Please select the DESlock+ licence type you wish to activate.

- Windows
- Mobile

bob@deslock.com requires a DESlock+ for **Mobile** licence.

Click **Next** to continue and choose from the available licences and generate an activation code.

If you have configured user

Send users Activation Code

Generate Activation Codes

bob@deslock.com requires a DESlock+ for **Mobile** licence.

Please choose from the available licences below.

Licence	Description	Available	Total
Mobile	IOS Perpetual	9	10
Mobile Subscription	IOS Subscription	9	10
Mobile Trial	IOS Trial (a)	10	10

This multi user licence can be used. **1** licence will be redeemed leaving the new available count at **8**.

Maintenance on this licence expires on Wed, Nov 12 2014

Back Generate Cancel

**Product types will only be shown for pools of licences that have been added to the Enterprise Server. If Mobile licences have not been added, then they will not appear in the list.*



Emails

Emails sent from the Enterprise Server have been updated with a new look and now use a template system. This means that the emails can be customised. For more information See: <http://support.deslock.com/KB144>

The default templates included are available in English, Polish, German, Dutch, French, Spanish and Japanese languages.

During activation, the email language can be selected for the user.



Any further emails sent from the Enterprise Server for the user will be in the selected language.



Active Directory Synchronisation

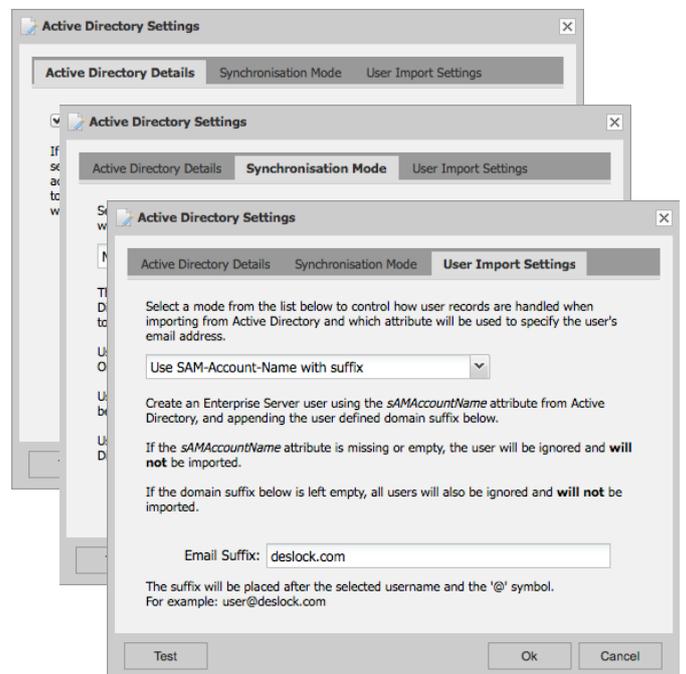
Previous versions of the Enterprise Server provides synchronisation with Active Directory, however only users that were configured with email addresses could be imported.

This release adds new options, to allow importing of users without email addresses from Active Directory. Email addresses can now be obtained from different fields or generated from other information.

The options are:

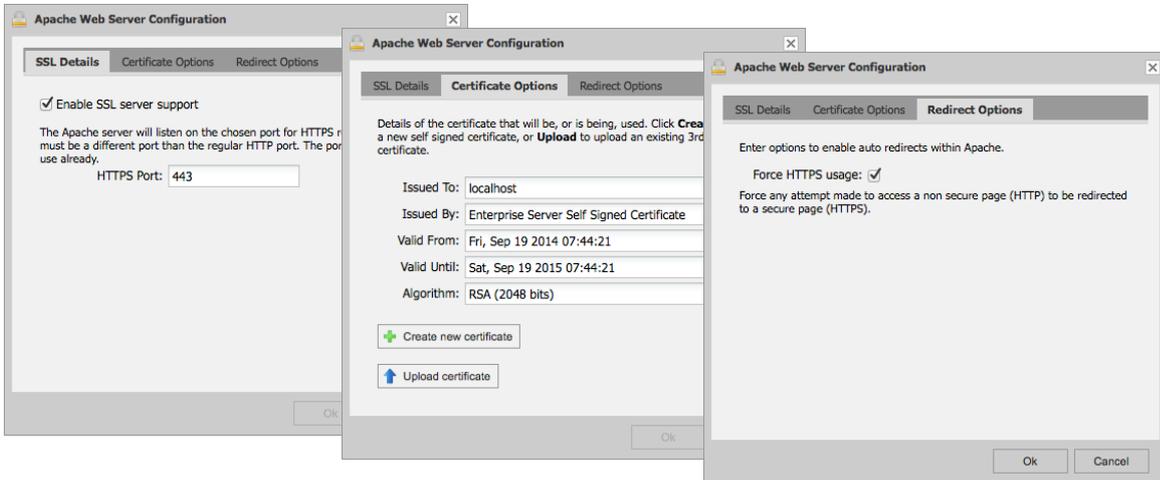
- Require E-Mail-Address (Mail) attribute
- Use User-Principal-Name attribute (UPN)
- Use E-Mail-Address (Mail) attribute if available
- Use SAM-Account-Name with suffix
- Use Common-Name (CN) with suffix

The Active Directory settings are available from the Enterprise Server control panel. They can be found in the Organisations section.



Secure Webserver Configuration (SSL/HTTPS)

Configuring a previous version of the Enterprise Server to use SSL requires manual configuration of the pre-installed Apache web server. This release provides a user interface to configure SSL, generate or import a certificate and force redirection to the secure HTTPS connection.



The Apache Server SSL Configuration is available from the Enterprise Server control panel. It is found in the Settings section.

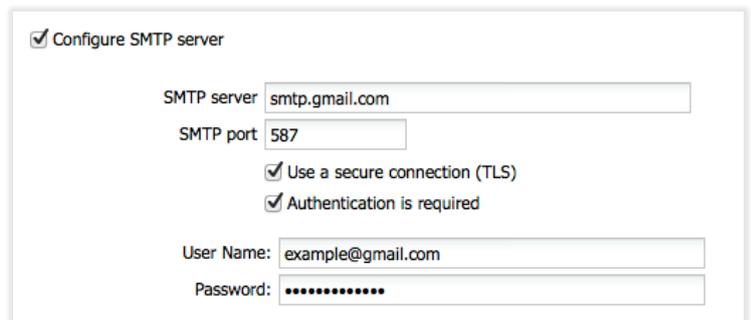


Please note that the Apache SSL Configuration should only be performed on an Enterprise Server pre-install running the version of Apache in the pre-install.

SMTP Support for Gmail / TLS

Support for SMTP servers has been improved.

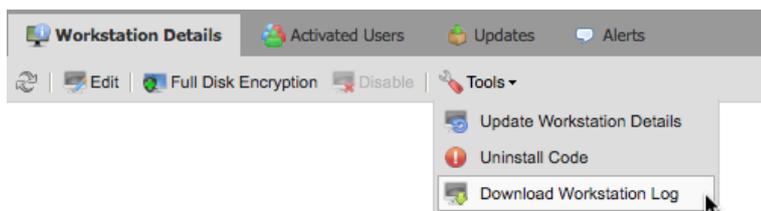
Emails can now be sent using Gmail or other email services that require TLS secured connections.



Workstation Information Logs

The workstation information returned from the DESlock+ Client to the Enterprise Server can now be viewed and downloaded. This can be useful for diagnostic purposes.

The Workstation Log can be downloaded from the Workstation Details window.



DESlock+ Enterprise Server - Workstation Log : DH-W7-EFI
Wed 24th September 2014, 10:59:15 BST

Enterprise Server Version	2.5.0
Organisation	Duncan Test
Workstation Name	DH-W7-EFI
Workstation ID	DC32629C-34ED-11E4-B156-000C29C6F59A
Description	
Workstation Type	PC
Uninstall Code	7HBH7-C92F6-XC35Q-QBGDW-RGKRG-7ZMZV-ZKHZMF
First Activated	Fri, Sep 05 2014 12:17:34
Created	Fri, Sep 05 2014 12:17:34
Created By	SYSTEM
Modified	Fri, Sep 05 2014 12:17:34
Modified By	SYSTEM

Workstation Status

- UpdatePending : true
- HasFDELogins : false
- HasAuthenticatedUsers : true
- PendingEncryption : false
- PendingDecryption : false

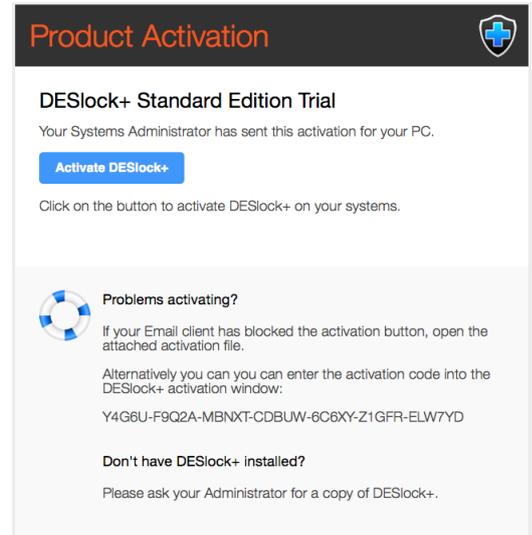


User Activation

This release improves activation of the DESlock+ Client by including a clickable button (link) in the activation email. To activate DESlock+ all the user has to do is click on the button and choose a password.



Some email clients may block the activation link, e.g. some web mail clients. If this happens, a file attachment is also provided. Double clicking on the attachment performs the same activation function. The activation code is also provided, as with previous DESlock+ versions this can be copied & pasted or typed into the activation window.



DESlock+ Mobile

The Enterprise Server now supports management of DESlock+ Mobile.

To use DESlock+ Mobile in managed mode, simply generate a Mobile activation code for a user, making sure to email it to them. DESlock+ Mobile can only be activated through the activation email; activation using a code is not supported.

Once activated the user has access to their encryption keys.



After activation, the Mobile device appears in a new Mobile Devices section in the Enterprise Server.



DESlock+ Mobile is available for Apple iOS devices and can be downloaded from the App Store. <https://itunes.apple.com/app/deslock+-for-ios/id880602467?ls=1&mt=8>

