DESlock+ Enterprise Server Manual

Table of Contents

1 Overview

The DESlock+ Enterprise Server is a browser based tool for the management of users and machines running DESlock+. It provides all the necessary functions to allow an administrator to specify security settings (Full Disk Encryption, Encryption usage and endpoint control) at the users' workstations. Data transferred between users and the Enterprise server can be kept on-site, or use a "cloud" based proxy server. All functional communications between the Enterprise Server and users are fully encrypted. Data held on DESlock+ Enterprise Proxy servers is also encrypted.

DESlock+ provides the user with full disk, folder, and email encryption, together with secure data deletion, encrypted virtual disks, encrypted archives, and removable media (memory devices) control. DESlock+ includes FIPS 140-2 Certified encryption algorithms.

The DESlock+ Enterprise Server allows the administrator to define the DESlock+ feature set for each user, to restrict or empower as necessary. Lost user passwords can be recovered with the Enterprise Server, even for Full Disk Encrypted workstations. Lost or stolen workstations can be remotely disabled, or set to self disable after communication with the server has been lost. The use of removable media (memory sticks) can be controlled to prevent Data Loss or imports of harmful programs.

See the Installation and Configuration Process Outline for a quick step by step guide to the stages required to set up your system

2 Features

- **Secure** – communication between the Enterprise Server and the users are encrypted using RSA. Data on any proxy server is also encrypted.
- **Resilient** – Server (local or cloud based) can safely self repair in the event of failure.
- **Flexible** – Single or multiple organisations, with either on site or widely distributed users.
- **Browser Based** with simple window display.
- **Easy to understand Interface**, with 2 main information areas (panels), showing the relationship, properties and in depth details of any selected user, key or grouping.
- **Multiple Keys** - Up to 64 different encryption keys can be used throughout the organisation.
- **Key Sharing** - Encryption keys can be shared between users and departments through Encryption Groups.
- **Administrator control** - 3 pre-defined administrator levels, each with differing control functions (System Admin, Admin and Helpdesk).
- **Roles** - Administrators can define custom roles for Enterprise Server access, allowing the delegation of simpler tasks to other users, without compromising the system security.
- **Team profiles** - can be propagated through the organisation simply and effectively.
- **Remote Full Disk Encryption** - initiation of Full Disk Encryption is performed remotely.
- **Wide Distribution of Clients** - Client workstations may be based locally or controlled via remote server, or through the internet.

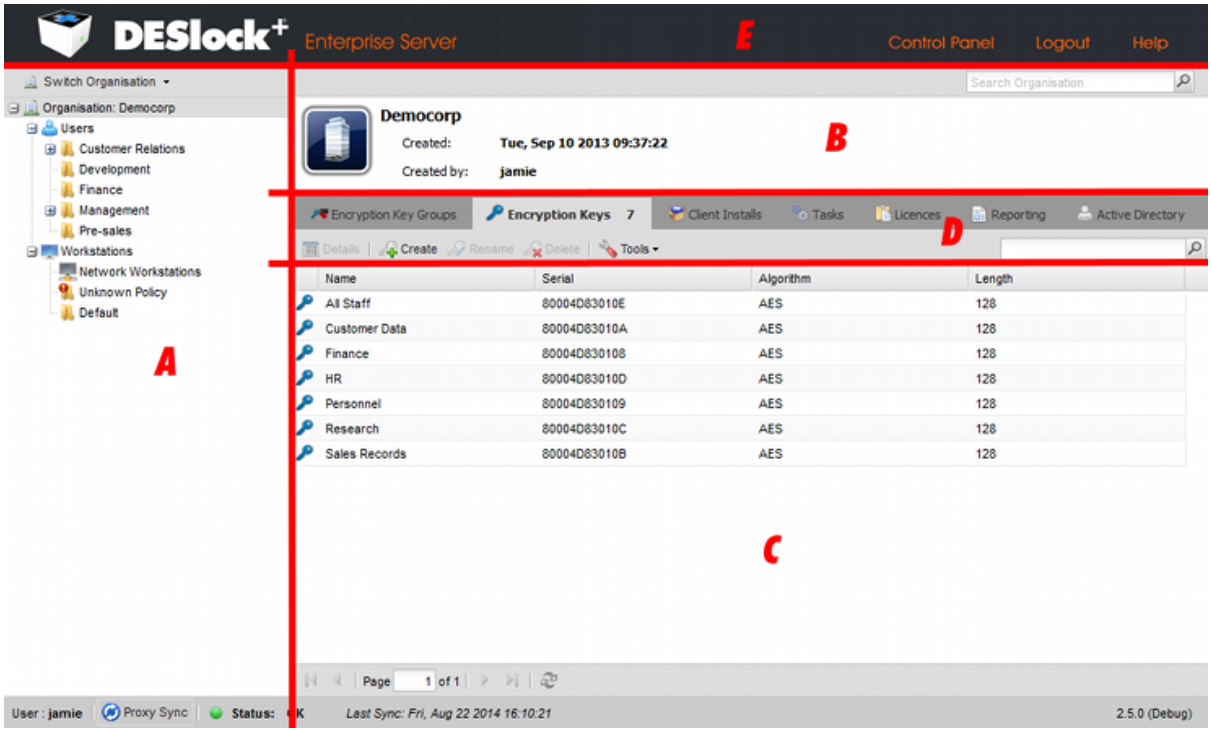
3 Interface and Main controls

Main Window

The Enterprise Server Interface has the following main information areas.

A) The Navigation panel displays the Organisation structure (management attributes, teams/users/ workstations etc). Selected item displays in more detail in panels B and C.
B) Subject title and basic information - panel displaying basic information on the subject selected in the Navigation panel.
C) Subject detail panel - displaying the details of the selected subject.
D) Tab and menu bar to select information displayed about the subject, and also to perform actions related to the subject (add, delete, move, generate etc.).
E) Main control bar to access the control panel, logout and help.

The information, buttons and options change to suit the Subject selected in the Navigation Panel. More details on these area's are below.



A) Navigation Panel

The Navigation panel (A), is where the structure and management of the organisation is displayed. This is where Organisation management is performed, and where the Teams (company structure) are displayed. Details on the Users, Workstations, Teams, Encryption Keys, Groups and Licences are shown in the right hand panels (in the B, C and D panels), depending on which item is selected in the Navigation panel.

The panel has two main display groupings, Organisation Management and the current selected Organisation Name (defined when the Enterprise server was installed) and structure – in this example the Organisation Name is Demo Ltd.

B) Subject Title

Panel B displays subject title and basic information about the item selected in the Navigation panel (A).

C) Subject Details

Panel C shows information based on the subject selected in the Navigation panel (A). The controls shown and the information displayed will be tailored to the type of subject selected. Users and workstations are displayed here.

D) Tab and Menu Bar

Depending on the subject selected in the Navigation panel (A), different tabs and menu options are displayed in the tab and menu bar, as described below.Panel C shows information based on the subject selected in the Navigation panel (A). The controls shown and the information displayed will be tailored to the type of subject selected. Users and workstations are displayed here.

E) Main Control Bar

This gives access to the control panel, allows you to Log out of the Enterprise Server, and also links to this help file. See Main Control bar and Control Panel for more details.

Tab Details

Depending on the subject selected in the Navigation panel, different tabs will appear on the menu bar, these are described below

Organisation Tabs

Selecting the Organisation root in the navigation panel will display the Encryption Key Groups, Encryption Keys, Tasks, Licences and Reporting Tabs on the Menu and Tab bar in the right hand panel. Depending on which Tab is selected the menu bar will change to provide suitable commands for that function.

Encryption Groups

Where encryption keys are grouped together for ease of control. New groups may be generated, keys added and removed.

Encryption Keys

Where new encryption keys are generated, stored, and renamed or deleted.

Client Installs

Where new versions of DESlock+ installs are stored. New releases are uploaded, then merged with a policy file for installation to a client machine, either manually or by pushing the install remotely.

Tasks

Holds a record of background tasks performed in the Enterprise server. (E.g. when multiple users are generated, this shows that the process has completed).

Licences

To use DESlock+ each user needs to have a licence, which are sold in multi user licence form. This allows the licences to be bulk purchased then distributed in a controlled manner by the system administrator.

Reporting

A selection of pre-defined reports allowing a simple record of information on the system to be viewed, created as a PDF or exported as CSV.

User Tabs

The User branch is found directly under the organisation, always as the first node. The various tabs will show Teams, Encryption Key Groups, Encryption Keys, Group Policy, Updates and Alerts, together with details of the selected tab item in panel C.

Users

Users are defined by email address and may be generated individually, in blocks (copy and paste) or by importing from Active Directory. Users within a particular team are controlled by the group policy at that level. See Team Users for more information. View User States for more information on the icons used for users and their corresponding states.

Teams
Teams are used to allow a logical representation of the organisation or function to be defined, which will simplify the allocation of policies and keys. The policies of each team generated is based upon the policies of the preceding level. The team inherits the policies and encryption keys of the parent team.

Encryption Key Groups
Displays the encryption key groups assigned to the Team currently selected. Groups may be added, moved or deleted as needed. Encryption Groups, and thus Encryption Keys also, will be inherited by any sub teams below that level.

Keys
Shows the Encryption Keys assigned to the selected team, through the use of the Encryption Key Groups.

Group Policy
Group Policy controls how DESlock+ functions and appears for a user (or client), which menus and controls they have access to. Group policy may operate in combination with the Workstation Policy that is on the workstation, or may override it completely.

Updates
Lists all the changes to users (force password changes, key file updates, etc) .

Alerts
Reports the status of various commands.

Workstation Tabs
The Workstation branch is found directly under the organisation, always below the Users branch. The various tabs will show Workstations, Teams, Encryption Key Groups, Keys, Workstation Policy, Updates and Alerts, together with details of the selected tab item in panel C.

Workstations
Workstations are added by installing DESlock+ on the workstation itself (using a downloaded or pushed merged install), which can then be activated with the Enterprise Server. See Workstation Installation for more details.

Workstation Policy
Controls how the Enterprise Server, user and workstation can interact with regard to the DESlock+ encryption and interfaces with external data sources. For example, time periods are defined after which the workstation may lock out access if it cannot connect to the server. As another example, users may not be permitted to read or write data to external media (USB memory devices).

Teams
Teams are used to allow a logical representation of the organisation or function to be defined, which will simplify the allocation of policies and keys. The policies of each team generated is based upon the policies of the preceding level. The team inherits the policies of the parent team.

Updates
Lists all the changes to workstation (full disk encryption commands, policy updates etc) .

Alerts
Reports the status of various commands.

The following two special nodes will be found under the Workstation branch.

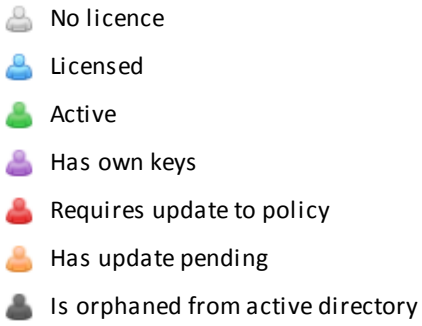
Network Workstations
Contains a cache of workstations discovered during a network scan. This list is obtained by the Enterprise Server machine by querying each domain or workgroup that is visible to it.

Unknown Policy
Contains workstations for which the installed policy is unknown. This could happen after for example if you are using an older DESlock+ client version that does not report its workstation policy to the server.

For certain tabs there will also be a search box available allowing you to locate specific information, either at the current level, or including sub-teams.

3.1 User States

User status is shown by colours, each signifying the operational state of the user. The colours are as shown below.



Light Grey
The user has no licence.

Only the user details have been defined on the Enterprise Server but cannot yet be managed. To manage the user, an activation code must be generated (which will licence the user if they are not already licensed) and they must then be activated upon a workstation.

Blue
The user has a licence, but is not active on any workstation.

The user has been defined and licensed, but the activation on a workstation has not yet been completed. The user must enter their activation code into a workstation, then the Enterprise Server must proxy sync to retrieve details of that workstation.

Green
The user is active and matches the Enterprise Server settings (clean).

The user is up to date and no changes need implementing. The settings shown in the Enterprise Server relating to the user, their encryption keys and the group policy of the parent team, match the settings the user has on each of their workstations.

Purple

The user user is active and clean, but has additional keys.

Extra keys have been defined for the user in addition to the normal key set inherited for the team. The purple colour implies the user is clean (see Green above) so no new Key-File needs to be issued. But the different colour signifies their special status in having non inherited encryption keys. See: User Specific Encryption Groups

Red

The user requires an updated Key-File.

Changes have been made to the group policy, or encryption keys, and the Enterprise Server is out of sync with the user's actual settings. You must send an update Key-File to reconcile the settings on the user's workstation with the settings in the Enterprise Server.

Orange

The user has an update pending.

An update has been posted to the user but have not yet been implemented at the client machine. This might be a change that removes an update state (Red), or it might be some other command. You can see the update in question in the Updates panel for the user. Please note, that the user will remain in this state until all updates have been processed, across all activated workstations. Or until superseded by a change that make the user as requiring an update (Red) again.

Dark Grey

The user was orphaned from an Active Directory.

The user was originally imported from an Active Directory, but the associated directory account has since been removed. A licence is still being used by this user so if this is now redundant you may delete the user after first taking any necessary steps to deactivate them from any workstations. However if the licence is still required, you can unlink it from the directory and the user will turn blue or green.

3.2 Workstation States

Workstation states are shown by a combination of two icon colours. Firstly the main colour of the workstation icon, followed optionally by the colour of second shield overlay icon to indicate Full Disk Encryption (FDE) status.

The main colours are shown on the left of the table below. The FDE colours are shown on the right. Please note the FDE icons could be applied to any main workstation state on the left.


Workstation not activated


Workstation activated and up to date


Workstation if fully Full Disk Encrypted


Workstation has update pending


Workstation is encrypting, or pending encryption


Workstation requires policy update


Workstation has reported an alert during FDE

Workstation States

Light Grey
Workstation not activated

The workstation has either not yet been activated by a user, or it was activated and has since been deactivated. The workstation cannot be managed by the Enterprise Server in this state, whether it has the DESlock+ software installed upon it or not.

Blue
Workstation activated and up to date

The workstation has an active user, and is up to date with the policy defined in the Enterprise Server

Orange
Workstation has update pending

The workstation has an active user, and is up to date with the policy defined in the Enterprise Server, but there is an update that has been posted to the workstation which has not yet been processed.

Red
Workstation requires policy update

Workstation policy has been changed on the Enterprise Server, and this is now out of sync with the policy currently on the workstation. The workstation requires an update to reconsile the workstation policy on the machine with the settings shown in the Enterprise Server.

FDE States

Green Shield
Workstation is fully Full Disk Encrypted

The workstation has completed a Full Disk Encryption process.

Orange Shield
Workstation is encrypting, or pending encryption

The workstation has been posted a Full Disk Encryption command but it has not yet reported completion. This could mean it has yet to start, or it is currently processing the command.

Red Shield
Workstation has reported an alert during FDE

The workstation is in the process of a Full Disk Encryption command, but it has paused and reported an alert. Check the Enterprise Server for further details. The most common cause an alert occurs is that the PC has been rebooted which has temporarily paused the Full Disk Encryption process.

3.3 Usage Examples

To find specific encryption key users

- Select the Organisation root node in the Navigation panel (A)
- Select the encryption keys tab on the Menu Bar (D)
- In panel C you will see a list of all available keys within the organisation.
- If you then select a key in panel C, and click the **Details** button (on the menu and tab bar)
- A new window will open, showing which groups contain the key and which users use the key.

N.B. Double clicking certain items can also be used instead of clicking the **Details** button.

To find user workstations

- Select the highest part of the management structure in the Navigation panel (A)
- you will be able to see the total number of users, workstations, teams, encryption key groups, keys, policy, updates and alerts that are defined at that level.
- If you wish to see all workstations below that point, click on the drop down arrow next to the search box on the menu and tab bar right hand side and check the "Include sub teams" box.
- You can also filter the displayed information by using the search field on the right of the menu bar, or using the drop down box to only show certain workstation types.

4 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 can be tailored to suit the requirements of different teams at a later time.

5. Licensing. Purchase licences to allow the licensing of users and activation of workstations.

6. Encryption Groups and Keys. Define the encryption keys and groups.

7. Teams. Defines the teams within the organisational structure.

8. Group Policy. This may be used to make adjustments in the team *level* policy. When the team is defined, it will take the current policy setting of the preceding level as its default. In the first instance, it will inherit the top level organisational policy. If required you can edit the team policy to reflect the permissions at that level. See Group Policy section for details.

9. Team Users. Defines the team users. Team users are defined by email address which can be entered singly or in blocks (copy and paste) as well as incorporating the import from Active Directory function – see the Organisation Manager section.

10. User Specific Encryption Groups. If required you may allocate the users specific encryption groups, other than those inherited from the team definition.

11. Create Workstation Install. Use the merge tool to create an installable DESlock+ package which is then sent to the workstations.

12. Workstation Installation. The user runs the install file on receipt (double click on the file), which will install DESlock+ and import the policy setting to that machine as one operation. The user then reboots the machine. During the Install, the machine will automatically register and report its status to the

Enterprise Server.

13. Activation Code. Administrator issues an activation code from the licence to the user which is sent via email.

14. Authentication. When the user starts their computer, they are prompted for their activation code (sent via email) and are then prompted to set their password. The user may then log into DESlock+ and use the features as defined by their administrator(or they may have been automatically logged in if enable and allowed by policy).

15. Workstation. The workstation will then appear in the Enterprise tool and may be encrypted.

16. Updates. From this point on, if the user details are changed (key groups added, policy changed) the status of the user will alter and they will require a new Key-File to be supplied. The administrator then sends the Key-File (keys and policy) to the user. Once the user has logged on, DESlock+ will automatically implement the policy settings for that user.

17. Full Disk Encryption. If required (and the licence includes FDE), once the workstation has been authenticated the administrator can initiate Full Disk Encryption for that machine. During this operation the administrator defines the login password for that user.

Before you start to install and configure the Enterprise Server, it will be of considerable benefit to plan out how you will define your organisation. You need to be aware of how it will be split into teams, what encryption keys and key groupings you will need, and what policies you have to set, both at workstation and group level. The more logically your organisation is defined, the simpler it will be to control and disseminate the security aspects of DESlock+

5 System Configuration and Installation

Preparing for first use

Installation

The DESlock+ Enterprise Server can be installed on any Windows XP (SP3) or later computer. The Enterprise Server should be installed in a location which is backed up to avoid potential loss of data.

Configuration

Before the DESlock+ Enterprise Server can be used, it must be configured. This is mainly performed during the MSI installation. That is, a database is created and the basic operating parameters defined.

You will need to supply:

- Installation folder location for the Enterpriser Server (or use default)
- Internet proxy settings (if they are required to access the internet)
- Sub folder location for access on the web server (eg http://localhost/dlpes)
- SQL Server details (name, username, password, database name)
- Enterprise Server details (organisation name, admin name, admin password)
- DESlock+ Proxy ID code

DESlock+ (latest release from website) will be required on all workstations, which will need registering with the Enterprise Server.

Next, review the Minimum System Requirements

5.1 Minimum System Requirements

The minimum requirements for the Enterprise Server are:

Host Operating System

- 1GB RAM - Or more, dependant on Operating System used.
- 30GB of drive space, minimum.
- 32 bit OS - XP SP3 or greater.
- 64 bit OS - Windows 2003 or greater.

Pre installed software

- SQL Server 2005 Express
- Apache 2.2 or IIS 6+
- PHP 5.3.x thread safe VC9

Other requirements

- Access to the internet on port 443 for connection to the cloud proxy and licensing servers

Optional

- SMTP account details

Client PC requirements

- Windows XP SP3 or greater
- CPU 2GHz+
- 2GB+ RAM
- 60GB+ Hard Disk
- Access to Server Proxy (HTTPS)

Next, define your Network Configurations

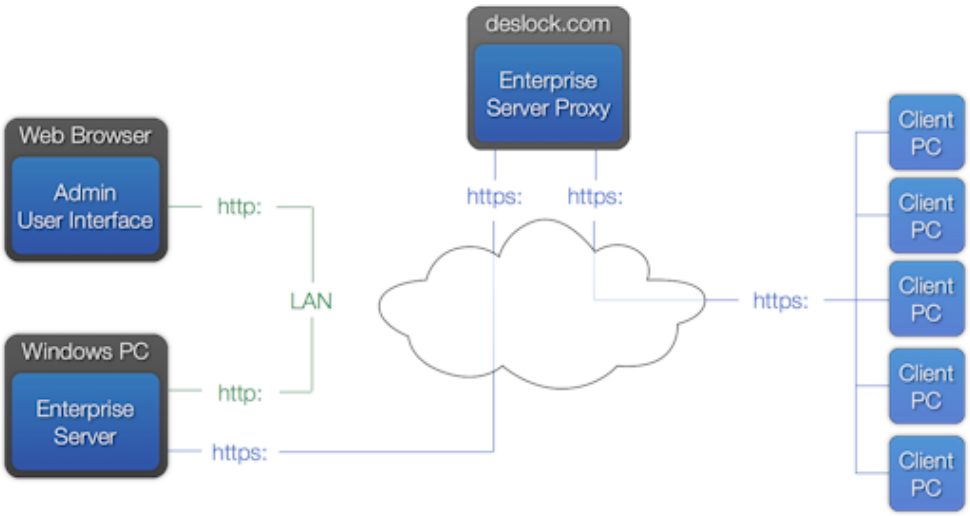
5.2 Network Configurations

Enterprise Server Usage Configurations

The Enterprise Server can be configured to operate in several ways, whichever is best suited to your organisational requirements. Any off site or cloud based data is always encrypted, as are the communications between the Enterprise Server and the client.

Standard Configuration

This configuration is the default recommended configuration. Client machines need only an outgoing connection to the internet, over HTTPS, to connect to our cloud proxy server. They need this only to receive updates, it is not necessary for normal use. The Enterprise Server similarly needs only a outgoing internet connection to our cloud proxy and licensing servers to post updates and licence new users. The Enterprise Server does not need to be continually running in order for client PCs to operate. So long as you have basic outgoing internet access in order to receive updates, there is no need to configure port forwarding, reconfigure firewalls, or maintain SSL certificates.



There are 4 essential components in the system

- **Admin User Interface** - This is the administration front end, accessed by a web browser from any PC with a local area connection to the Enterprise Server itself. So, as an Administrator you can use the Enterprise Server package from any location that has access to the PC/Server that is hosting the software. The web browser can be on any PC, even a client PC, or the Enterprise Server PC. We currently support Internet Explorer (8 or greater) or Firefox.

- **Enterprise Server** - The main system database containing the details accessed by the admin user interface. This also controls the communication with the server proxy. This must be installed on a Windows based computer, satisfying the minimum system requirements (Windows XP SP3+ or Windows Server 2003+)

- **Enterprise Server Proxy** - the communications interface between the Enterprise Server and the client PCs. All data on the server proxy is encrypted. The server may be physically on your site, or a remote system residing in the 'cloud'. DESlock Ltd have a secure server available for your use if required. The server proxy can also be on the same on site PC as the Enterprise Server

- **Client PC** - The users workstation. Multiple users can use the same machine, each with a different account and different encryption keys. Client PC's can be based anywhere with access to the server proxy. So, depending on network organisation, the client may have LAN or internet access.

The standard configuration as shown above, uses our own server proxy - 'cloud' based - for your secure communications. The components are the four outlined above. There are minimum requirements for these components specified in System Requirements.

There are no real differences between the Performance, Security or Reliability of the other configurations, they are included purely to give you possible set up scenarios.

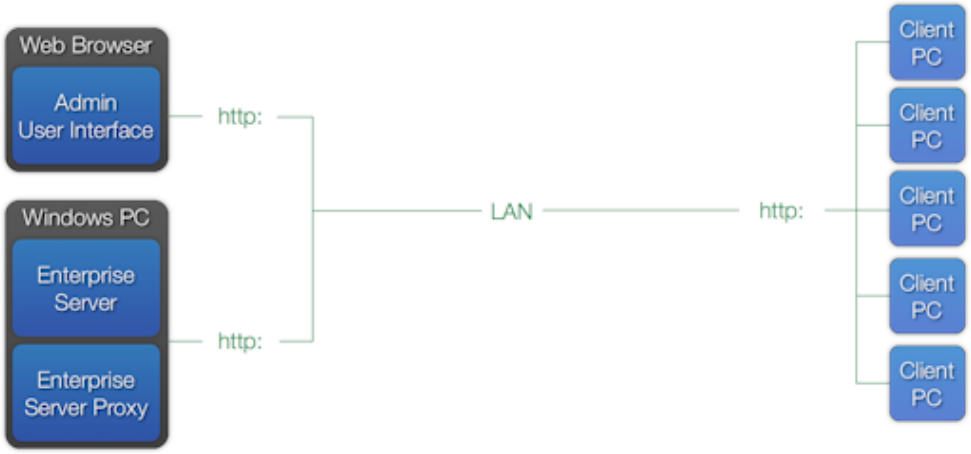
Alternate Configuration

If your client machines do not have internet access to connect to the DESlock+ cloud proxy, you can use a Local Area Network installation. Please note however that the Enterprise Server itself will still require internet access to access the licensing server. However client machines can operate without internet access.

Once you have decided on your Network configuration (which elements of the supplied software you will use, or which of your own), proceed to the Software Installation

5.2.1 Local Area Network

In this scenario, rather than using the cloud service provided by DESlock Ltd, it is possible to host and use an alternative Enterprise Server Proxy server within you own network. In this instance, all traffic is restricted within the network. You will still require a internet connection for licensing users, but all Enterprise Updates will only stay within the defined local network. You must still provision and maintain the proxy server, and supply and maintain an SSL certificate if you wish to use a secure connection.



5.3 Pre-requisite Install

To install the Enterprise Server a pre-requisite install is available. The complete Enterprise Server installation including Microsoft SQL Server, Apache Web Server and PHP 5.3 is relatively simple, essentially just a few clicks.

This will install the Enterprise Server and the necessary programs. Once installed, the wizard will offer the option to launch the Enterprise Server in the default browser. The Enterprise Server can be accessed using all modern browsers.

5.4 Setup Wizard

Once the Enterprise Server has been installed, launching the console in a web browser will start the configuration wizard. It is required to complete this wizard before the Enterprise Server is fully operational and can be used.

The wizard will guide you through all necessary steps required to configure the Enterprise Server for initial login.

5.5 Login

To start the DESlock+ Enterprise Server, you will need to login. Navigate to the network location where your copy of the DESlock+ Enterprise Server has been installed. Depending on your browser, you will see a screen similar to the one below. Enter your username and password and click Log in.

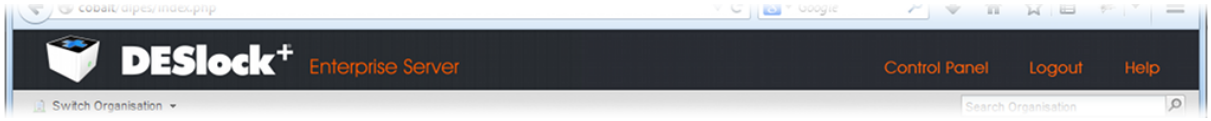
First Use

Once you are logged into the Enterprise Server you will need to familiarise yourself with the interface, set up the workstation and group policy, define the structure of your organisation. This process is outlined in the Installation and Configuration Outline section and in more detail elsewhere in the manual.

6 Main Control bar and Control Panel

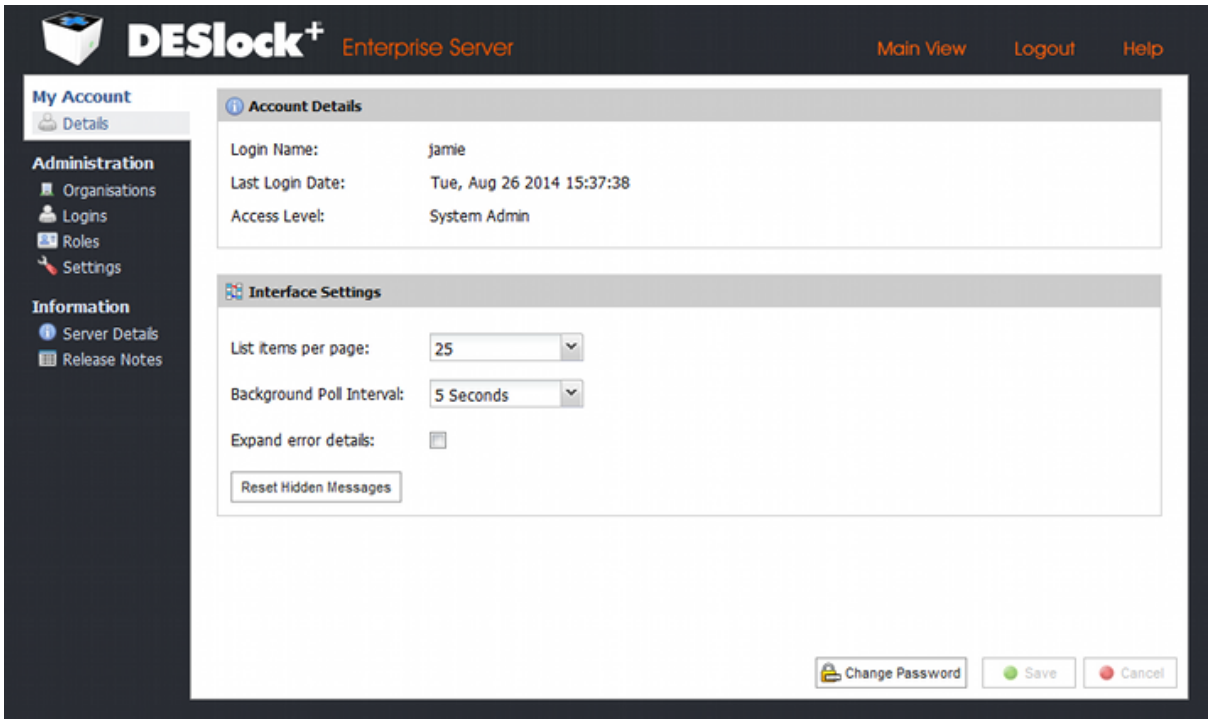
Main Control bar

The main control bar provides access to the Control Panel, Logout and Help. It also includes (if applicable) options to switch organisation and a search facility allowing the current organisation to be searched on specific key words.



Control Panel

The full Control Panel is only available if you have the correct settings made available in your defined role. There are three types of standard user roles available (system administrator, administrator and helpdesk), a system administrator can generate new roles and assign these to users.



With system administrator rights you can see all the options as above. My account (all roles), administration (organisations, logins, roles and settings) and information.

The control panel gives you access to My Account, Administration and Information, each of which is described in more detail in the linked sections.

Logout

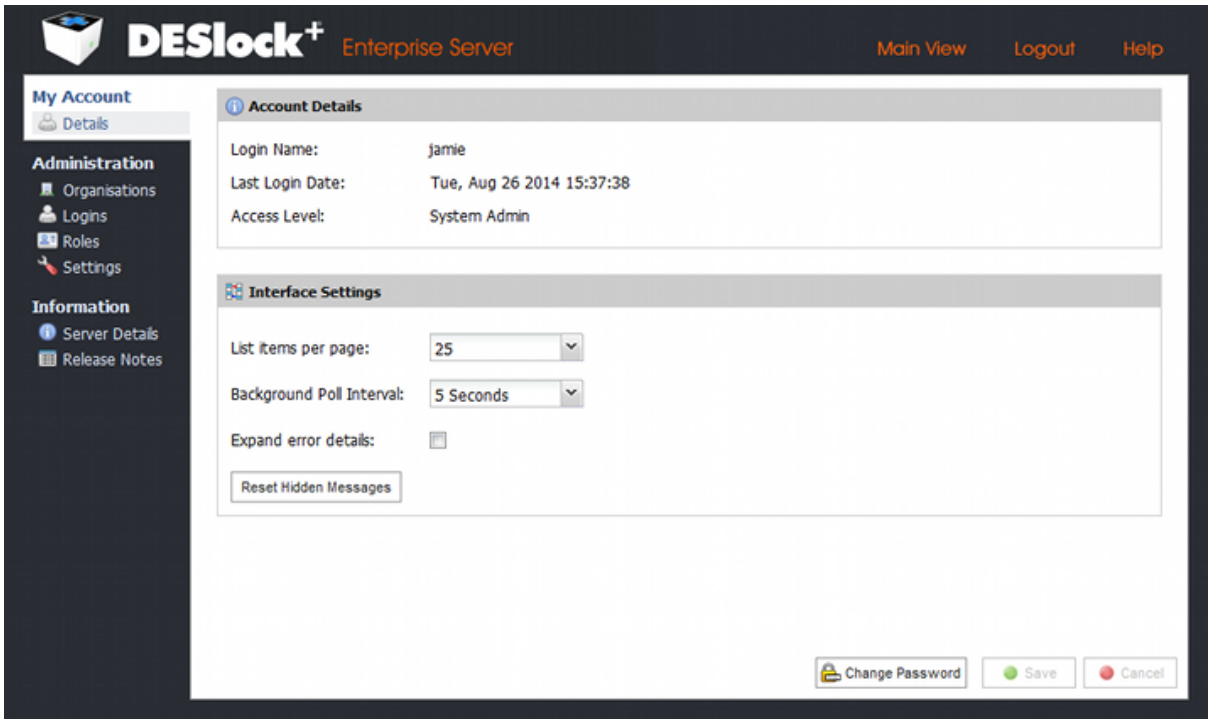
This will logout of the Enterprise Server and return the user to the Login screen.

Help

This launches the help system (this).

6.1 Control Panel Settings

The control panel has three sections on the left hand panel of the display, My Account, Administration and Information, as can be seen below.



My Account

Shows details of your account plus a few interface (display) settings that can be changed. Not all users can change/view settings. For more details see My Account

Administration

In the Administration section, a system administrator can manage and create organisations, users, roles and modify the settings of the Enterprise Server. For more details see Administration

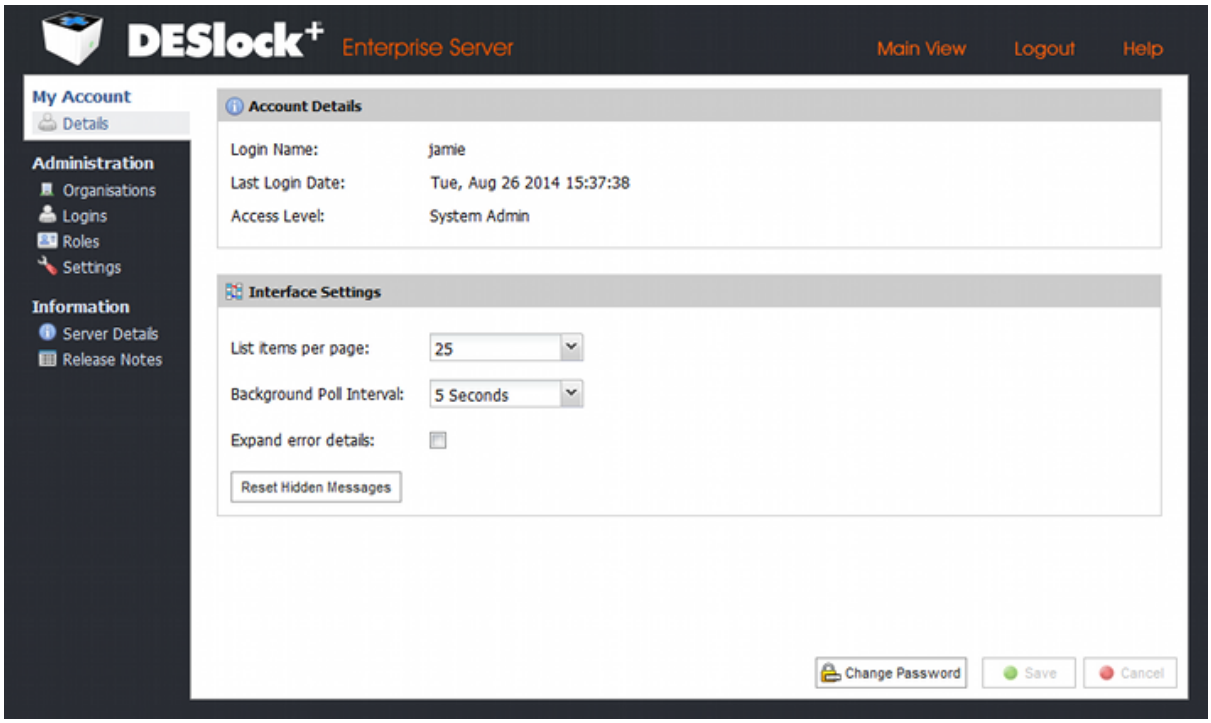
Information

In the Information section, the administrator can view the file versions of the Enterprise Server. There are no settings that can be changed. For more details see Information

6.1.1 My Account

Details

The Details panel displays details of the currently logged in user.



The only user settable features are:

- List items per page - How many items are displayed per page
- Background Poll interval - How frequently the system refreshes
- Theme - Basic colour theme setting (Blue or Gray)
- Expand Error details - expands the details of errors displayed.

All users have access to their user tab in the control panel, but not all users can change/view settings.

Once you have made your changes, you must click the Save button to commit the change. Click the Cancel button to cancel the changes and revert to the previously saved settings.

Change Password

If you wish to change your Enterprise Server login password, click the Change Password button at the bottom of the screen. Please not the password must adhere to the password policy that has been specified.

6.1.2 Administration

The administration panel allows access to various settings relating to the overall operation of the Enterprise Server.

These are described in more detail in the chapters linked below

- Organisations
- Logins
- Roles
- Settings

6.1.2.1 Organisations

This panel allows control of organisations. Organisations can be created or destroyed. Organisation settings can be changed at an individual organisation level.

Create new Organisation

To generate a new organisation

- Click the **Add** button at the bottom of the panel.
- Enter the new organisation name in the Add organisation window.
- Click Create.

Delete

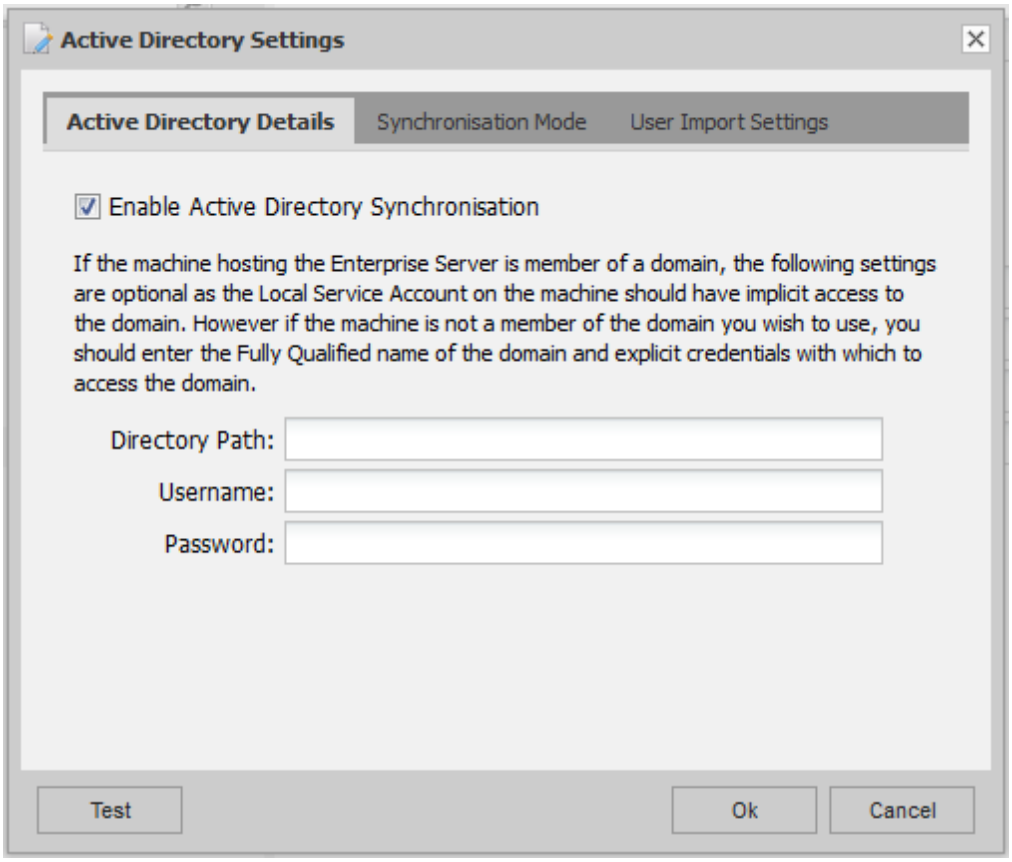
To delete an organisation, highlight the organisation and click the **Delete** button.

Edit Name

To change the name of an Organisation, select it and click the **Edit Name** button on the lower right hand corner of the details panel.

Active Directory Settings

To edit Active Directory Settings for an Organisation, select it and click the **Active Directory Settings** button on the lower right hand corner of the details panel. You can enable or disable Active Directory integration by checking the box. You may then enter any of the option settings or change the synchronisation mode. There are three pages of settings to fine tune the import mode.

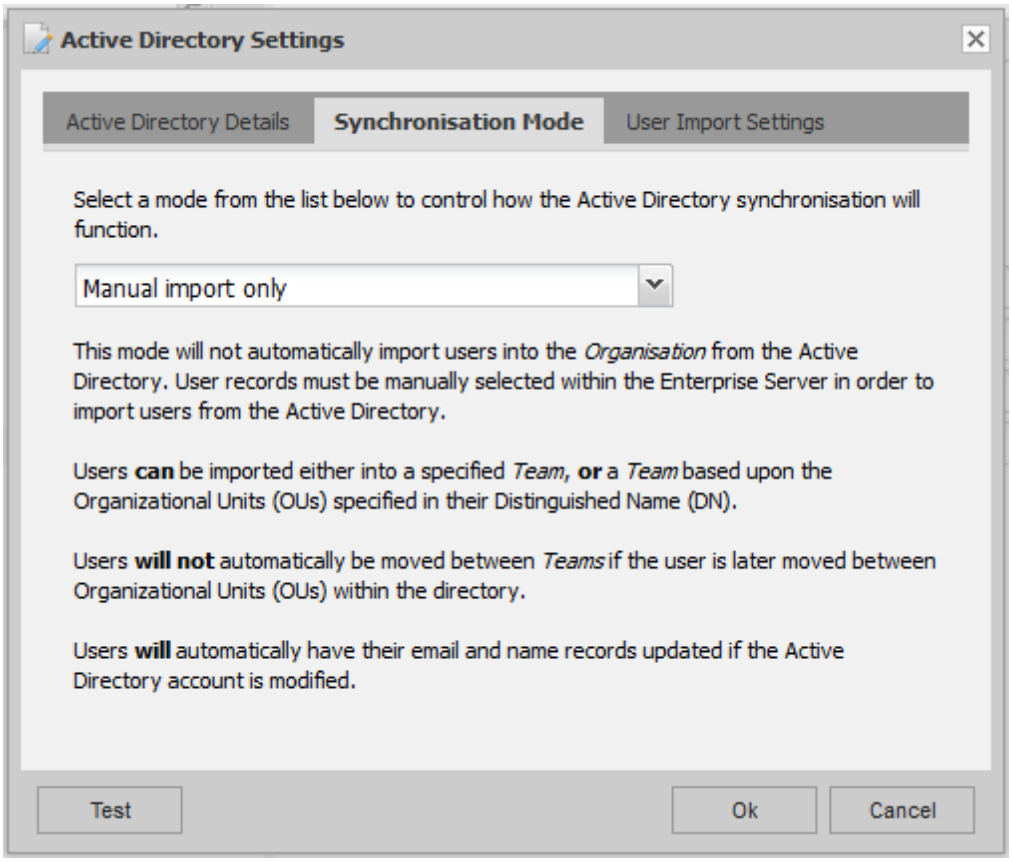


If the machine running the Enterprise Server is a member of an Active Directory, it may be sufficient to simply enable support. However, if the machine is not a member of a domain, or you wish to synchronise only with a specific object, you can enter the server name, distinguished name and user credentials as required.

Synchronisation Mode

The synchronisation mode defines how the synchronisation will operate, and whether it will run

automatically in the background, or if it requires user intervention. The effects of each option are given on the dialog when the selection is made.



The options are:

Automatic with Team Import

Full Automatic Import will automatically import any users from the Active Directory into the Enterprise Server, using the Organisational Units (OUs) the user is in to determine the team name in the Enterprise Server. Additionally, if users are moved between OUs in the directory, they will also be moved between teams in the Enterprise Server. Username and email changes are also applied to the Enterprise Server users if the name is changed in the directory.

Basic Automatic Import

Simple Automatic Import is similar to the full automatic mode, but the OUs are ignored and users are simply placed in the root of the organisation. They can be subsequently moved within the organisation, and they will remain in their specified Teams even if they are moved within the Active Directory. However, username and email address changes will still occur.

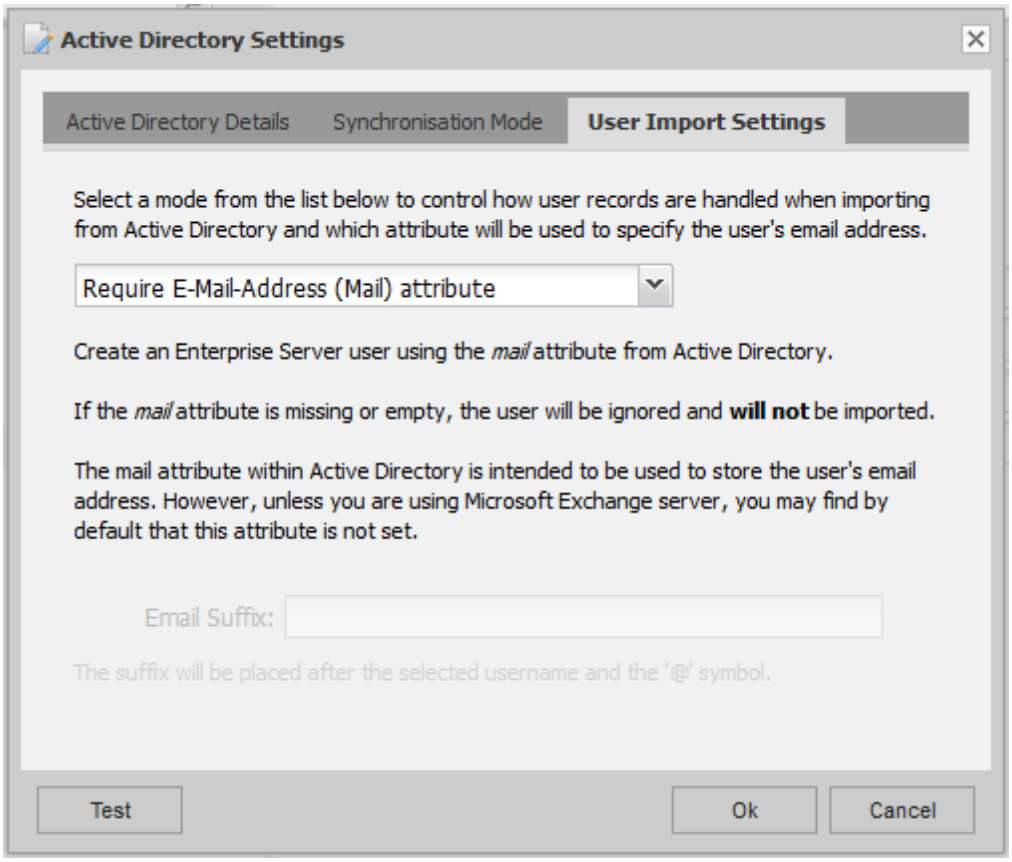
Manual Import Only

In manual mode, no users are automatically imported into the Enterprise Server, and it is up to the user to import users to link them. Users can be moved within the organisation, and they will remain in their specified Teams even if they are moved within the Active Directory. Also username and email address changes also occur automatically for any manually linked users.

User Import Settings

By default, all users within the Enterprise Server are licensed using an email address and thus by default the Enterprise Server will use the mail attribute within Active Directory for the email address within the Enterprise

Server. However, in cases where the mail attribute has not been configured, other attributes can be used instead of the email address (such as the UPN) or can be combined with some user defined domain suffix.



6.1.2.2 Logins

This panel allows control of logins to the Enterprise Server console. Logins can be created, renamed or destroyed, login settings can be changed, and access to indiviual organisations can be granted or denied.

Selecting a login will show various options, such as:

- Assigned role,
- Currently logged in status,
- Last login date
- Last login host
- Password age (last password change date)
- Account status (locked, must change password etc).

Create Login

To add a new user, select Logins;

- Click Create.
- Provide the login name, password, password confirmation and the role (based on an existing role, use the dropdown arrow to select).
- Click Create.

The new user will be added.

Logout User

If a user is currently logged in, you may forcibly disconnect them by clicking the logout button. This will expire their session causing the user to be redirected to the login page. Any operation they are currently performing may be aborted.

Set Password

If a user has forgotten their password, or you wish to change it for some reason, it may be reset by clicking the **Set Password** button. By default this is a System Admin only permission so may not be available for all users. to change your own password, you should use the Change Password feature in the My Account section of the control panel.

Edit Login

To edit a login, select the login and click the **Edit Login** button.

- To change the login role, select an available role from the list.
- To lock an account, so the user cannot login, check the **Account Locked** box. To unlock a lock account, clear the check.
- To force a user to change their password before they can login, check the **Must Change Password** box. At their next login attempt, the user will be forced to change their password before login is granted.
- To exempt the password from password age checks, as defined in password policy, check the **Password never expires** check box.

Modify allowed organisations

Once a user has been created, you will need to define the organisations they can access, unless they are a system administrator who will automatically have access to all organisations.

- Select the user whose access you wish to change (additional information will be displayed for the user)
- In the right hand panel you will see a list of allowed organisations (none will be displaying for a new user)
- Click Grant
- The "Grant Access to Organisation" selection window will appear.
- Select the required Organisation and click Grant.
- Organisation will be added to the users permitted list.

- If required, once you have a user selected you can also deny access to an organisation, change the authorisation level of the user or change their password.
- If the user is defined as a system admin role, they automatically have access to all organisations.

Delete Login

If required you can also delete an existing login.

- Select the login to be deleted.
- Click Delete

6.1.2.3 Roles

The Roles panel allows creation and modification of a role based permission system, to fine tune access to Enterprise Server features.

To assist in granting the correct level of access to users, there are a number of standard built-in roles available which cannot be modified. New Roles can be created with specific access rights by system administrators. There are 3 standard user roles available (System Administrator, Administrator and Helpdesk) which are described below. Also, a System Administrator can generate new roles (based on any existing roles) and assign these to users which provides flexibility to the system.

Standard Built-in Roles

System Administrator

The system administrator has full access to all features and functions of the Enterprise Server. They can generate new organisations, add new users and configure the appearance of the displayed information. Through the settings control they can change internet access, security requirements and SMTP server settings. They can add, modify and delete any operational function (encryption keys, groups, teams, users, workstations, etc), and add new roles for user access. In effect, they are administrators for the entire system and have full access to the entire system.

Administrator

An administrator can do all that a System administrator can, with the exception of various system based tasks (they cannot add organisations, create Enterprise Server logins, add new ES roles, or copy encryption keys to another organisation). In effect, they are administrators for the specifically defined organisations, but cannot modify system settings.

Helpdesk

A Helpdesk user has limited access to Enterprise Server functions, they can change their own password and can view, but not change other details concerned with the daily operation of the system.

Creating new Roles

To create a new Custom Role, select Administration from the control panel, then Roles, click New and in the sub window select an existing role to base the new one upon.

Amending the Role permissions

Once generated, you can add and remove the permissions as required. Select the role in the Custom Role window (centre panel at the bottom, below), this will then display the permissions associated with that role. To Add (or remove) permissions, click the **Add Permissions** or **Remove Permissions** buttons. In the sub window select those functions to be added (or removed)

6.1.2.4 Settings

The settings panel contains settings designed to improve security and performance. Some may also be necessary for the Enterprise Server to function correctly.

Enterprise Server Login Security

Change or update the policies enforced on Enterprise Server login passwords.

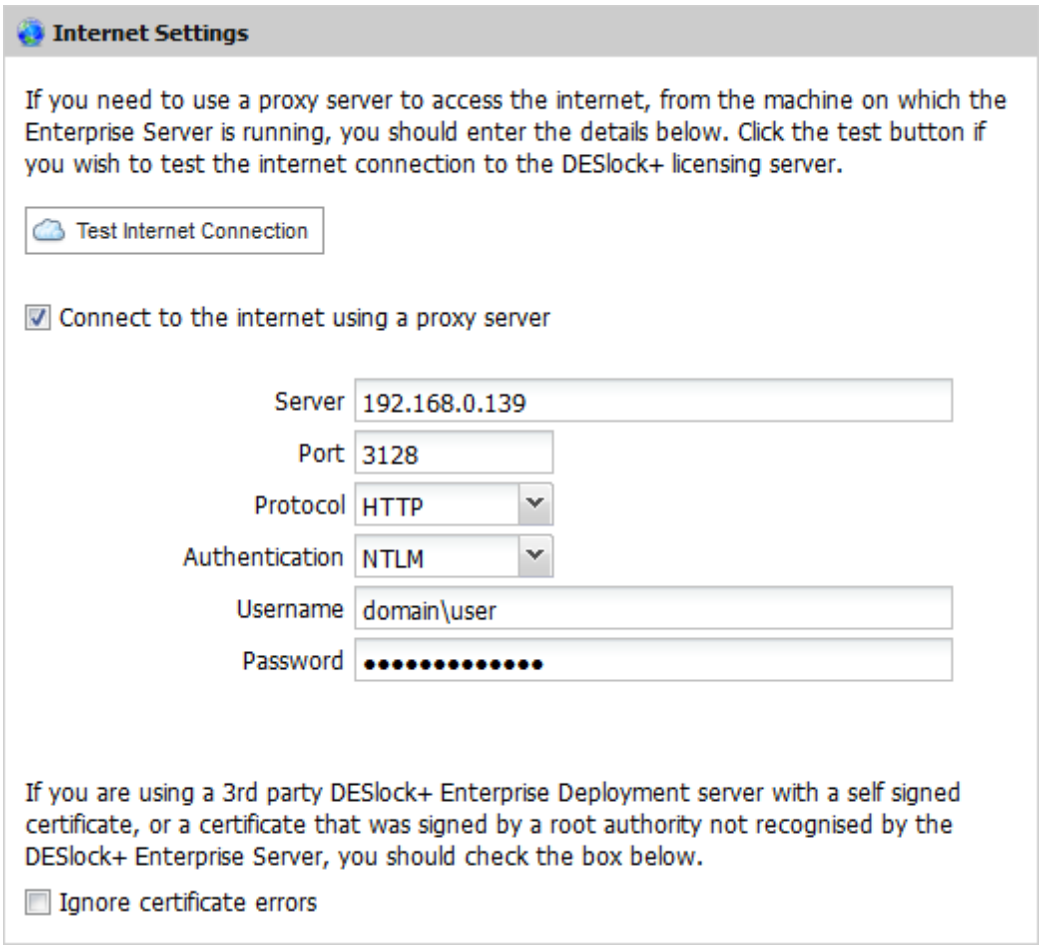
Please note this is only for logins with access to the Enterprise Server itself, and is not related to the client password policies accessible via Group Policy.

Internet Access

Settings required for internet access from the Enterprise Server machine. By default the Enterprise Server requires access to **licensing.deslock.com** and **stratus.deslock.com**, over port 443 (HTTPS). It may also require access to a third party proxy server if you are using one instead of the cloud proxy service.

Here you can enter details of any proxy service you may have. You can also allow the Enterprise Server to ignore certificate errors for SSL connections in the event a 3rd party proxy is using a self-signed certificate, or a certificate signed by a non trusted root certification authority.

If you are in doubt over any of these settings, please refer to your network administrator.



Mail Settings

If configured, the Enterprise Server is capable of sending emails to users to notify them of certain information. This includes activation codes for users, and FDE login details.

If you wish to enable this support, you should enter details of your SMTP server here, along with a reply address.

If you wish to test the email settings, ensure they are entered and saved correctly and enter a test address and click **Send a test email**.

Auto Update Checks

By default, the Enterprise Server will automatically check for new versions of the software and display a message when a user logs into the Enterprise server. If you wish to disable this functionality, you can clear the tick from the **Enable Auto Update Check** option.

If you have inadvertently chosen previously to ignore a version, you may reset the setting so you are notified of the new version again.

Background Timers

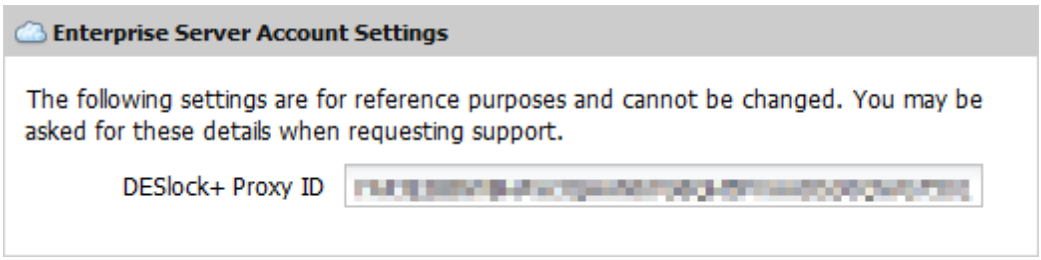
The Enterprise Server is designed to poll for external changes on a regular basis. This can be either when checking for status reports from client workstations on the proxy server, or when checking the list of users on the Active Directory (if configured).

You may change these values to either decrease the frequency of checks in a low use environment, or increase

the frequency so the Enterprise Server can automatically respond to changes much faster.

Cloud Proxy Settings

DESlock+ Proxy ID. This is supplied by DESlock when first installing. Also referred to as the "Cloud ID". This is displayed for reference purposes only, as it may be useful when contacting support.



6.1.3 Information

The Information panel gives basic Enterprise Server information

Server Details

Brief details on the file versions and operational status of the system.

Release Notes

The information on the release status, fixes applied and known problems for the currently installed version.

7 Policy Settings

There are two policy setting controls that are available for fine tuning the operation of DESlock+ Enterprise Server, **Workstation Policy** and **Group Policy**.

Workstation Policy

Controls how the Enterprise Server, user and workstation can interact with regard to DESlock+ encryption and also interfaces with external Data sources; basically the physical environment of the workstation. This policy applies when the user is not logged into DESlock+, or is not yet activated on the workstation. Group Policy (below) may override some setting in Workstation Policy when the user has activated DESlock+.

See: Workstation Policy

Group Policy

Controls how DESlock+ functions and appears for the user, which menus and controls they have access to and the software environment.

See: Group Policy

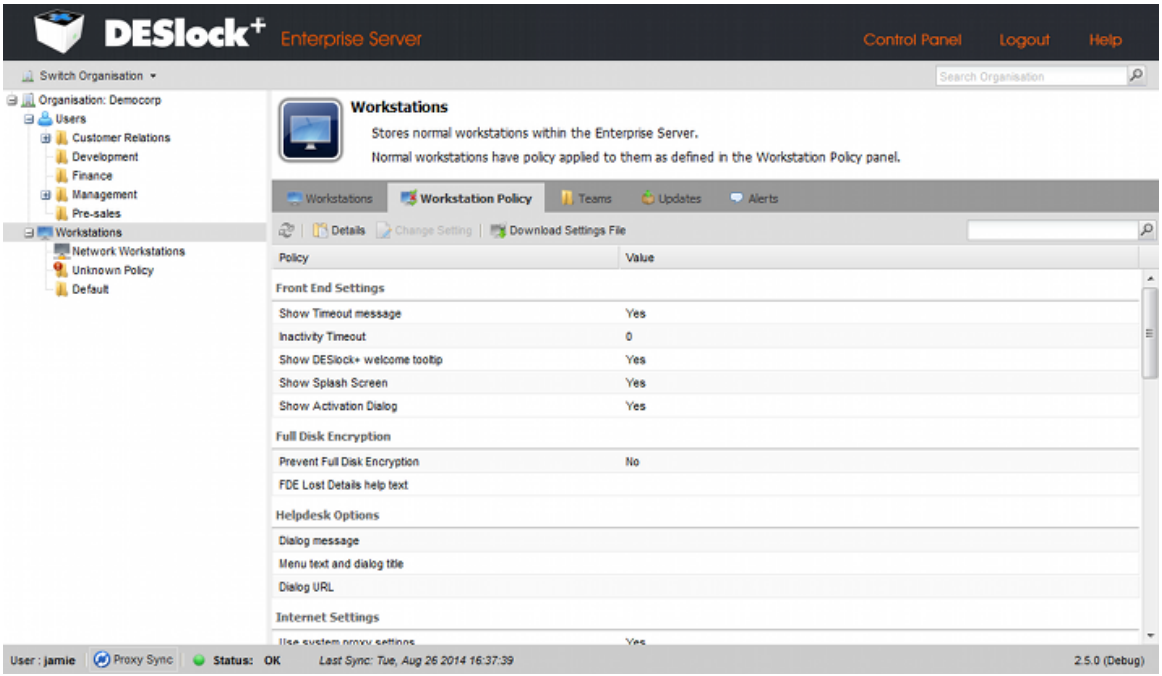
7.1 Workstation Policy

Workstation Policy is defined within the teams below the Workstations branch in the main view.

Workstation Policy controls how the Enterprise Server, user and workstation can interact with regard to the DESlock+ features and how the user can interface with external Data sources. For example, the network path to the Enterprise Server is defined here, display message text is defined, permitted length of time for “out of contact with Server” periods, and external media permissions. For full details of all the settings and their use see Enterprise Server Policy Setting PDF's (Workstation and Group)

Workstation Policy definition

To define a Workstation policy, simply create a new team under the Workstations branch. Any workstation moved into this team can be pushed the updated Workstation policy, and modifying the policy in this team will not affect any other teams that do not inherit their policy from this team.



To edit a Workstation policy, select the Team on the left and then go to the Workstation Policy panel on the right. You can edit any setting, and optionally download a registry file if you wish to adopt a standalone workstation or update an old client.

Please note that changes to workstation policy are not automatically distributed to workstations.

7.2 Group Policy

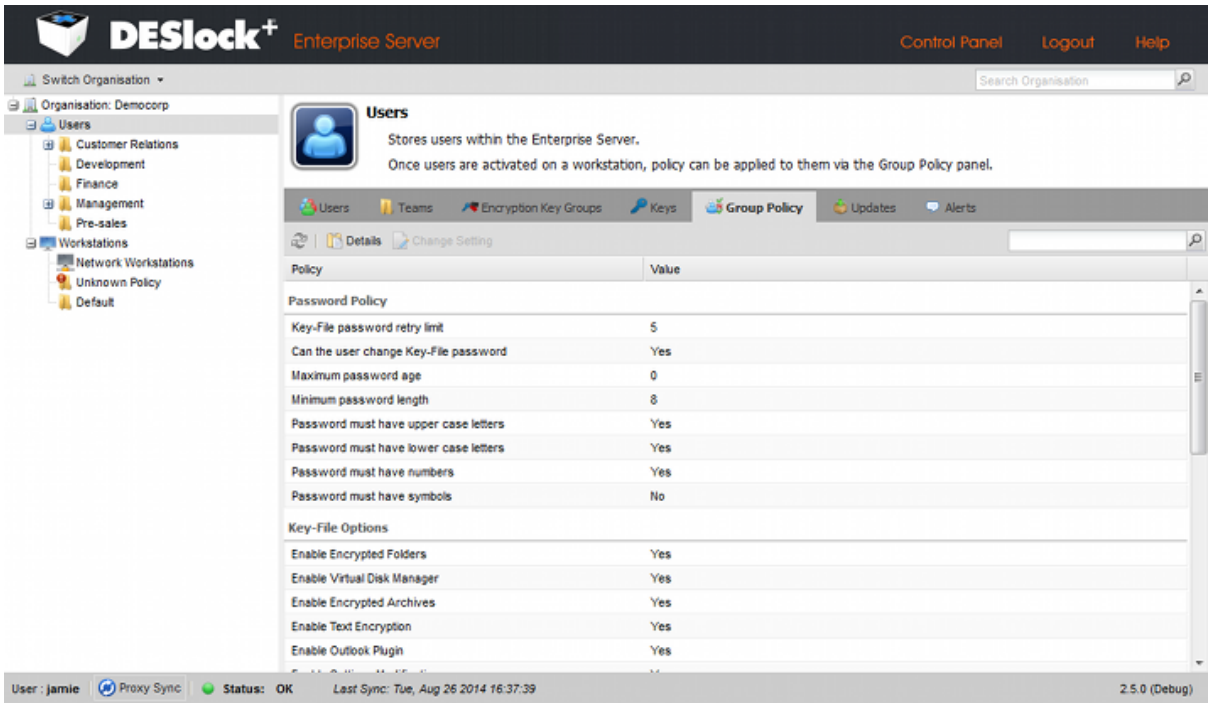
Group Policy is defined within the teams below the Users branch in the main view.

Group Policy mainly controls how DESlock+ functions and appears or the user with the controls and menus they have access to.

Group Policy definition

To define the initial Group policy, select the root of the Users branch in the Navigation panel, then select the Group Policy tab in the subject detail panel.

Important Note. Group policy can be different for each level of an organisation with each subset inheriting the settings of the level above. So for example a Sales department has Group policy settings based on the Demo organisation, but these can be altered to better suit the requirements of that department.



Additional detail of each policy setting can be shown by clicking the "details" button.

Group Policy Changes

To change a setting, highlight that setting in the policy list and click on the “Change Setting” button in the menu bar. This will display a window for the policy under amendment, a drop down box for the permitted settings and the same brief description of the function of the setting. See below. Select the response you want or define the text required and click OK to save the new setting.

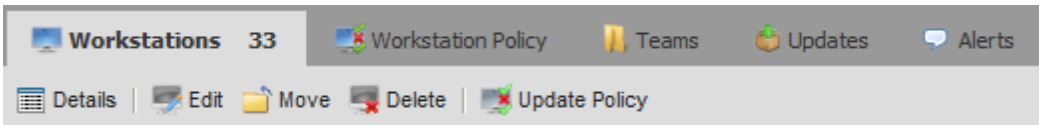
Please note that changes to group policy are not automatically distributed to users.

7.3 Updating Policy

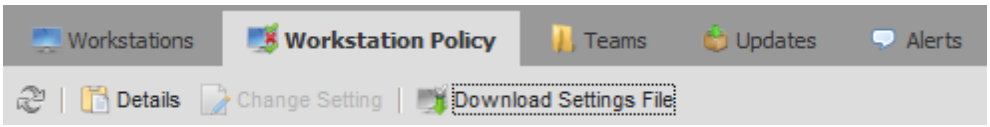
When you first define and install a new user on a client computer, the workstation and policy files will be supplied as part of the installation and authorisation package you send to them. Any changes to either Workstation or Group Policy made after this point will have to be sent to the client or workstation for it to be applied.

Updating Workstation Policy

There are two methods to updating workstation policy, depending on the version of client software. If the client is using DESlock+ 4.5.0 or later, you can simply select the workstation from the Team panel, then click the Update Policy button. This will post out the new policy which the client will apply automatically.



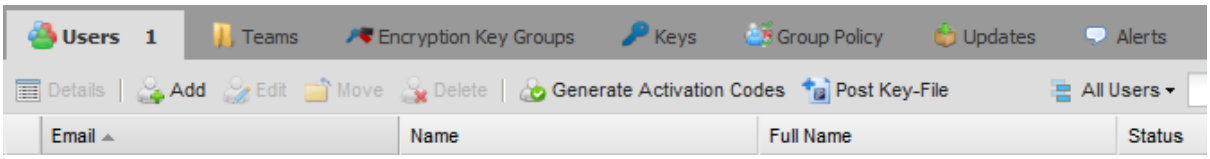
If you are using an older client, prior to 4.5.0, in order for the policy to be changed you will need to manually apply a registry merge (.reg) file. Select the team containing the workstation, then select the Workstation Policy file. Select "Download Settings File". This is saved locally then has to be sent to the users for implementation by an admin user. Depending on your browser, you may have to select the download location of the file.



You may also wish to use the downloaded policy file if you wish to adopt an already existing standalone client.

Updating Group Policy

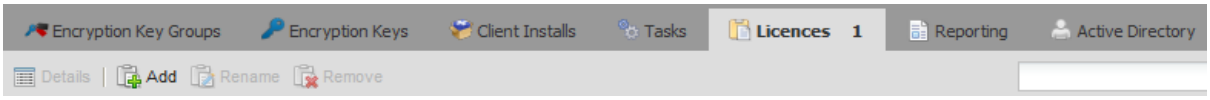
If you make any changes in Group Policy in any team after the team members have been defined and installation files created, the status of the affected users will alter (colour change) and they will require a new Key-File to be supplied. The administrator will need to post a Key-File (which contains encryption keys and group policy) to the users affected. Once the user has logged on, DESlock+ will automatically implement the policy settings for that user.

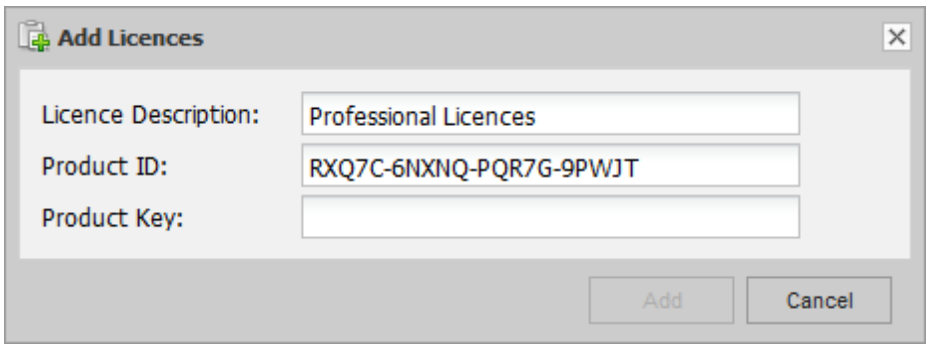


To post a Key-File update select the team in the Navigation panel, then select the 'Users' tab in the tab bar. In the subject detail panel select the user to be updated, then click Post Key-File. The update will be sent by the Enterprise Server to the user via the cloud proxy server. This is covered in more detail in the Updates section.

8 Licences

- Purchase a multi-user licence with enough licences for the required number of users.
- Upon purchase, the The licensing server will send an email to the registered users email address for the multi-user licence and will include a Product ID and a Product Key.
- In the Enterprise Server select the Organisation root, then the Licences tab and then select Add. See below.





- In the" Add Licences" window enter your own description for the licences followed by the Product ID and a Product Key received

- Click Add.

The licence and relevant codes will be entered into the Enterprise Server database and will be used to create valid activation codes (in conjunction with the DESlock+ Licensing Server) as you issue licences from the Enterprise Server. These codes will then be used to activate your users as required.

Licences

Licences have to be redeemed against a multi-user licence purchased from DESlock.

Before you can issue a licence you have to define the teams and users (and their relevant Policy Settings). See Activation Code Generation for more details on issuing users with licences.

9 Encryption Groups and Keys

There is no order in which Encryption Key Groups or Encryption Keys need to be created. In this example we are creating Encryption Keys first.

Encryption Keys

In the Navigation panel, select the Organisation root then the Encryption Keys tab.

To add a new key click 'Create' in the menu. Give the key a name and select an algorithm (Blowfish, 3DES or AES) and click Add.

Encryption Groups

To create an encryption group, select the Organisation root in the Navigation panel then select the Encryption Groups tab. To add a group click create in the menu bar.

Next, In the Create Encryption Key Group window, add the name of the new group and click Add. The new group will then appear in the Encryption Group Tab.

Add Encryption Keys to the Group

You may then add the required keys to the group. Select the Organisation root in the Navigation panel, then the Encryption Group tab. Select the required group in the subject panel then click Details. You can also double click the desired group which will open the detail panel as before.

In the Encryption Key details window, click Add, then in the Encryption Key Store window select the keys you want and click Add.

The keys will be added to the group and the status of any team member that has that Encryption Key group will change (to Red) which will indicate that the user requires an updated Key-File is posted to them.

9.1 Encryption Key import

Encryption keys may be imported into the Enterprise Server from external DESlock+ Key-Files. For example, if an organisation already has DESlock+ Encryption keys in use within their security system it will be logical to use the Enterprise Server to control and distribute these existing keys more effectively. This can only be done if the keys are first imported into the Enterprise Server.

To do this the Enterprise Server and the Encryption Key holder have to be able to exchange data securely. This is necessary so that the key holder's key can only be used by the Enterprise Server - if the exchange is intercepted/lost or stolen the key contained in the file will be unobtainable (encrypted) and of no use to them. Key transfers are secured by RSA encryption.

The process is as follows, in simple terms:

- The Enterprise Server Administrator requests the key from the key holder by generating a special request file

(with a file extension of .DLR)
- The key holder then issues the key to admin, using the request file (.DLR) to encrypt the key. This results in the generation of an update file (.DLU)
- The key holder sends this update file to admin.
- Admin updates their Key-File with the update, which adds the key just received from the key holder.

For the Enterprise Server the process is as follows:

1. In the Navigation window, click Organisation Management, then the Encryption Key tab followed by **Download Request File**.
2. After being present with a file-save dialog
3. Click OK and the file will be saved where specified (depending on your browser) with the name KeyRequest.dlr.
4. Send this file to the holder of the key you require (by Email, or over your network).

5. To issue a key, the holder of the required key will follow the steps below:
   Right click on their DESlock+ icon in their Notification Area (also know as System Tray) and select the Key Transfer option.
   Select "Issue a Key to another user", then click next
   Select the request file sent from the Enterprise Server administrator.
   Select which key to issue.
   Specify the terminator code for the key being issued. This must not be set at 0, as this will prevent the key being used by the Enterprise Server. A value of 1 will allow the key to be distributed within the Enterprise Server but not issued by any of the Enterprise Servers clients. A value of 2 or more will allow the key to be issued onwards by the Enterprise Server's clients, assuming the transfer of keys is permitted by their policy settings.
   Specify the location of the update file and complete the process.

   The saved Issue file (.DLU) is then sent by the holder to the Enterprise Server by email/file transfer.

6. In the Enterprise Server, import the file by selecting Organisation Management, then the Encryption Key tab and by by clicking Import Update File. Specify or browse to the location of the Update file (.DLU) and click upload. The key transferred will be added to the Encryption Keys database.

10 Teams

Teams are used to allow a logical representation of the organisation to be defined which will simplify the allocation of policies and keys. When a team is created it takes its attributes from its parent (the selected item in the navigation pane) for its initial settings. So whichever part of the organisation you have selected in the left hand pane, will be used as a template for the team created - in other words the current team's policy settings and encryption key groups will be created in the new team.

Teams will often represent the physical function of the team members, their location or a combination of the two. The purpose of the team is to provide an additional method of allocating and controlling encryption keys and hence access to data.

If there is an organisation structure already defined, select the logical parent of the team you are adding. This Parent's attributes (Group Policy and Encryption Key Group) will be used as the template of the new team.

Creating a Team

To create a team, select an existing team in either the Users or Workstations branch. Select the Teams tab and click Create to generate a new team.

In the Create Team window, enter the required team name and click 'Create'. The new team will be added as a child of the originally highlighted team.

If you view the key groups or policies (with the tabs) for the team created, the display will show if any encryption group or policy has been inherited from a parent. To change these policies see Group Policy

Inherited Policy

Once the team has been defined you can then amend the group policy for that team following the same steps as noted before (See Policy Settings), but making sure you have the correct team selected in the Navigation panel. This will allow you to have different policy settings for different groups if necessary. Make any changes to the policy before you create or license any team users, as the policy settings are distributed as part of the licensing package sent to the user. Any changes made to the group policy after the team members have been defined will require a new Key-File to be supplied to the affected users.

10.1 Moving Users or Workstations

To move a user or workstation between teams, first select the parent team in the Navigation panel, then the 'Users' or 'Workstations' tab and then select the item to be moved. Click the 'Move' button on the menu bar.

Then in the window that is shown select the team that the user is to be moved to and click 'Move'.

The user will be moved to the new team and the user's status may change to red and "requires update". This will happen if the destination team has a different group policy or a different set of encryption keys. If both are the same however, then the user should retain their existing state. Update any dirty users by posting a Key-File which will replace their existing keys and group policy to match the new team. For details of Key-File updates see Updating Policy.

Please Note, moving a user and removing their existing encryption keys may leave encrypted data on their computers that they are unable to access (EG data encrypted with keys unique to their previous team). If required their encryption key groups can be edited to provide any necessary access to the Encrypted data and an updated Key-File posted.

10.2 User Specific Encryption Groups

Once the user has been defined and licensed their encryption groups may be amended. It is not possible to leave any inherited groups, only to add (or delete) extra groups.

First select the team in the Navigation panel followed by the 'Users' tab and then select the user.

Click the 'Details' button and a new window will open with the user details.

In the user detail window, click the Encryption Key Groups tab. All current key groups that the user belongs to will be shown with any inherited ones shown in green.

Joining an Encryption Key Group

To add a new key group select "Join Group" and in the sub window select the group to join - then click OK. The new group will be added and a new Key-File will need to be posted to the user.

Leaving an Encryption Key Group

To leave a key group (non inherited groups only), in the user detail window, click the Encryption Key Group tab. All current key groups the user belongs to will be shown with any inherited ones shown in green. To remove a key group, select the key group to be removed and select "Leave Group". In the sub window, click the check box to confirm the action, then click 'Leave'. The encryption keys will be removed from the user once a new Key-File has been posted to the user.

10.3 Active Directory

If you are using Active Directory, it is possible to have the DESlock+ Enterprise Server monitor the directory and add, remove and modify users automatically based on changes in the directory.

To enable this functionality, see the Organisation Active Directory Settings in the Control Panel.

Managing Active Directory Users

If Active Directory sync has been configured, and if the user has permissions to view the panel, an Active Directory panel will be displayed in the Organisation Management section of the Enterprise Server.

User States

The users may be displayed with the following icons:


The user was found in the active directory, but nothing exists in the Enterprise Server user list


The user exists in the Enterprise Server user list and is linked to an Active Directory user


The user exists in the Active Directory but it is being ignored. Therefore it will not be imported into the Enterprise Server, even in automatic modes


The user exists in the Active Directory but it is in a different organisations. This user cannot be imported into this organisation


Any user with a highlight mark, which could be displayed with any of the icons above, means it is new since the last directory synchronisation

User Options

Re-Sync

Re-sync happens automatically on a timer. However, clicking the button will wake the timer and cause the re-sync to begin immediately. The tool tip displayed will inform you when the synchronisation is complete, it could take some time depending on the size of the directory.

Quick Import

Quick import will import the user/s into the organisation, using the user's current OU as the destination team. Note that unless you are in full automatic mode, the OU is only used for the initial import and the user will not be moved during subsequent synchronisations.

Import to Team

Import the user/s into a user specified destination team.

Ignore User/Unignore User

Ignore the user, or clear the ignore flag.

Removing a User

Removing From the Directory

If a user is removed from the Active Directory, during the next synchronisation event the following will occur.

If the user is not yet licensed, they will be removed immediately from the Enterprise Server.

If the user is licensed, or activated on a workstation, then they will be marked as an orphan user in the Enterprise Server. This can be seen by a dark user icon.

If you no longer wish to retain the licence for this user, you may delete them from the Enterprise Server and the licence will be released and can be re-used.

However, if you wish to retain the licence, you can unlink the user from the directory using the button on

the user card. This will turn the user back into a normal user and the icon will revert to the previous state.

Removing From the Enterprise Server

If you delete a linked user from the Enterprise Server, it will mark the corresponding active directory user as ignored.

11 Adding a Workstation

The process of adding a workstation and activating a user on it is outlined below and also shown in detail in the linked chapters. The Enterprise Server is not designed to allow direct addition of workstations, but rather workstation will automatically be added as a result of a user activating on the workstation.

1. Create workstation install.
   - To do this, upload a DESlock+ Client install to the Enterprise Server (unless the latest one is already there).
   - Make sure workstation policies are as required for the new workstation.
   - Download a merged install for the workstation. This includes the DESlock+ Client software and Workstation policies

2. **Workstation Installation**.
   - Supply the Installation package to the workstation.
   - Install the package on the workstation.

3. Activation Code Generation.
   - Generate a user activation code for the workstation.
   - Supply the activation code to the user.

4. Workstation Activation.
   - When the workstation is booted after installation the user is required to enter the activation code.
   - The activation wizard will communicate with the Enterprise Server for validation and supply the user with their Key-File and group policies.

5. Synchronisation.
   - Once both ends of the system (Client workstation and Enterprise Server) have synchronised, the workstation and user will appear in the Enterprise Server as "normal"

6. Future Updates. From that point on, any group policy or Key-File changes will need to be posted to the activated user.

11.1 Create Workstation Install

To create a workstation install you need to have a client install (DESlock+) merged with a set of workstation policies. The client install needs to be loaded in the Enterprise Server and the workstation policies need to have been amended to suit your organisation. For details on how to amend your workstation policies, see Policy Settings. The client install and workstation policies need to be merged together by the Enterprise Server to form a complete installation package.

Upload Client Install

If there are no client installs already loaded into the Enterprise Server you need to upload one. If you have a client install supplied by DESlock you should use that, if not go to the DESlock website (www.deslock.com) and download the latest version (32 or 64 bit, depending on your requirements).

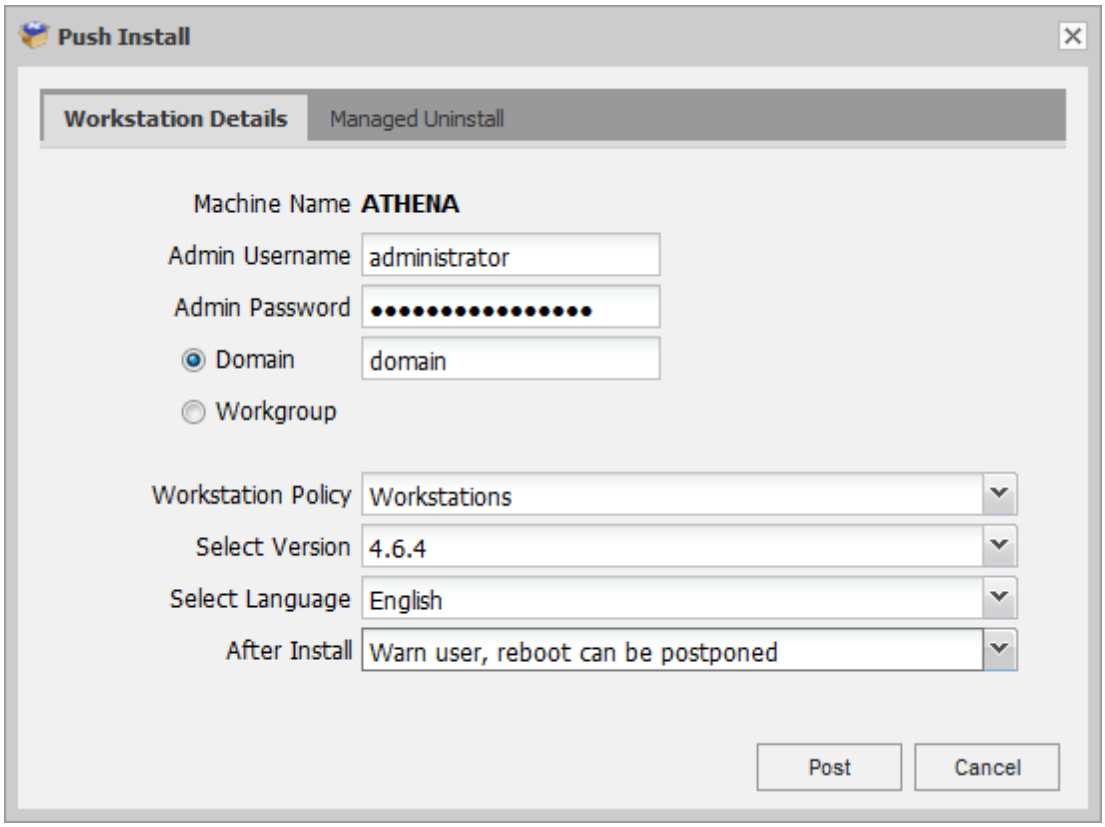
To upload the install, select the Organisation root in the Navigation panel, then 'Client Installs' on the tab bar and click 'Upload'. In the sub window browse to the files location and then click upload. The Install will then be listed in the Installs Library.

Create a Merged Install

To create a merged install there are two possibilities. Firstly you can download the MSI and install this manually, or distribute it to the client PCs using a 3rd party installation manager. Alternatively if the intended destination client PC is connected to the local network, you can remotely push an install to it directly from the Enterprise Server.

Push Install

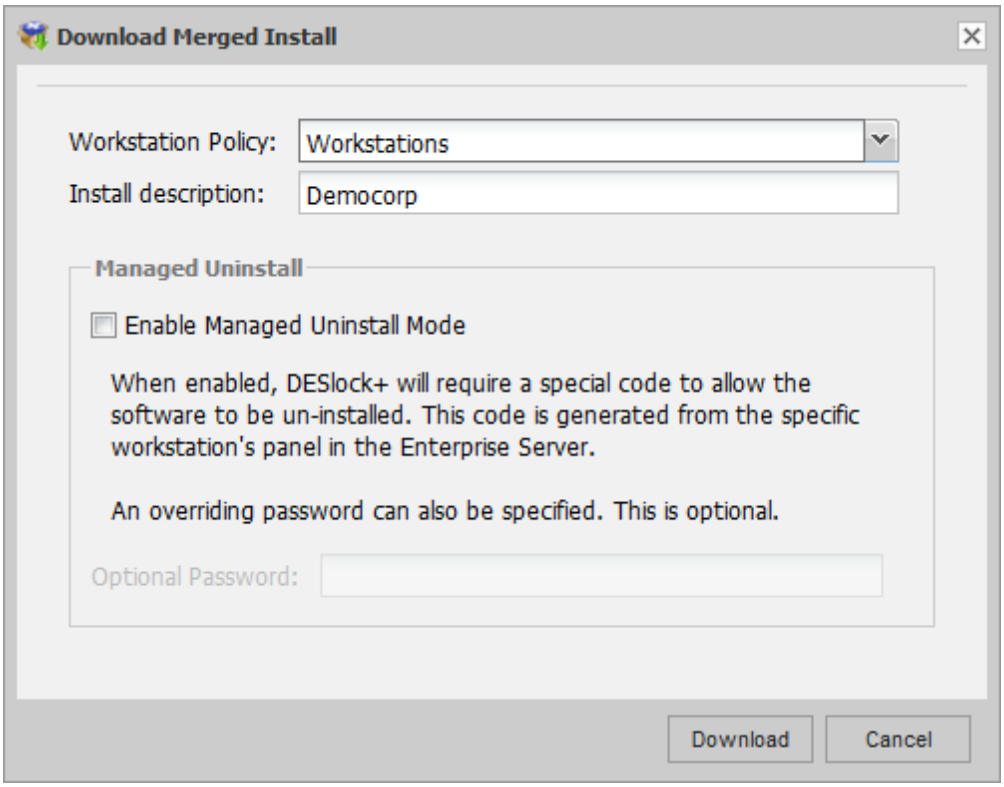
From the Network Workstations node under the Workstations branch, ensure the desired destination workstation is listed. Perform a network rescan if necessary. or manually enter the machine as required if it is not listed. Click the "Push Remote Install" button.



Enter a username and password for a user with local administrative privileges on the destination workstation. If you have selected multiple workstations, the account must have local administrative privileges on all selected workstations. Select a workstation policy, a version of the client software and a language for the install. The DESlock+ software required a reboot of the system after installation so you may also choose the action that is taken if a user is actively logged into the workstation at the time of the install. The setting only applies if a user is logged into the system at the time. If no user is currently logged into the workstation, then workstation is automatically rebooted without prompt.

Downloaded Install

From the Client Installs panel, select the required install version, click "Download Merged Install". You have to specify which workstation policy you require to use (if you have multiple policies defined). Click "download" and the file will be saved. Depending on your browser you may have to specify a location or it may default to "downloads". This merged install can be supplied to many different workstations.



You can also select to enable a managed uninstall with an additional optional password which will prevent the user from removing DESlock+ from their system unless they have the correct codes.

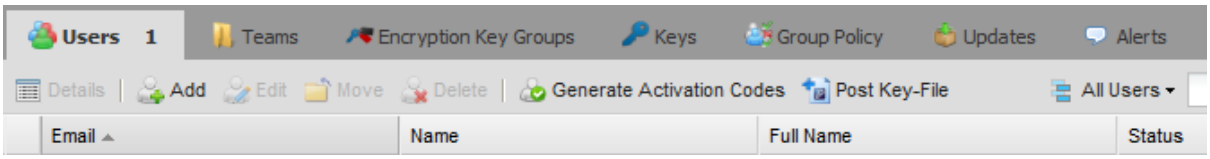
The system creates an installable MSI which can be supplied to the client for installation.

Now see Workstation Installation for details on the installation process.

11.2 Activation Code Generation

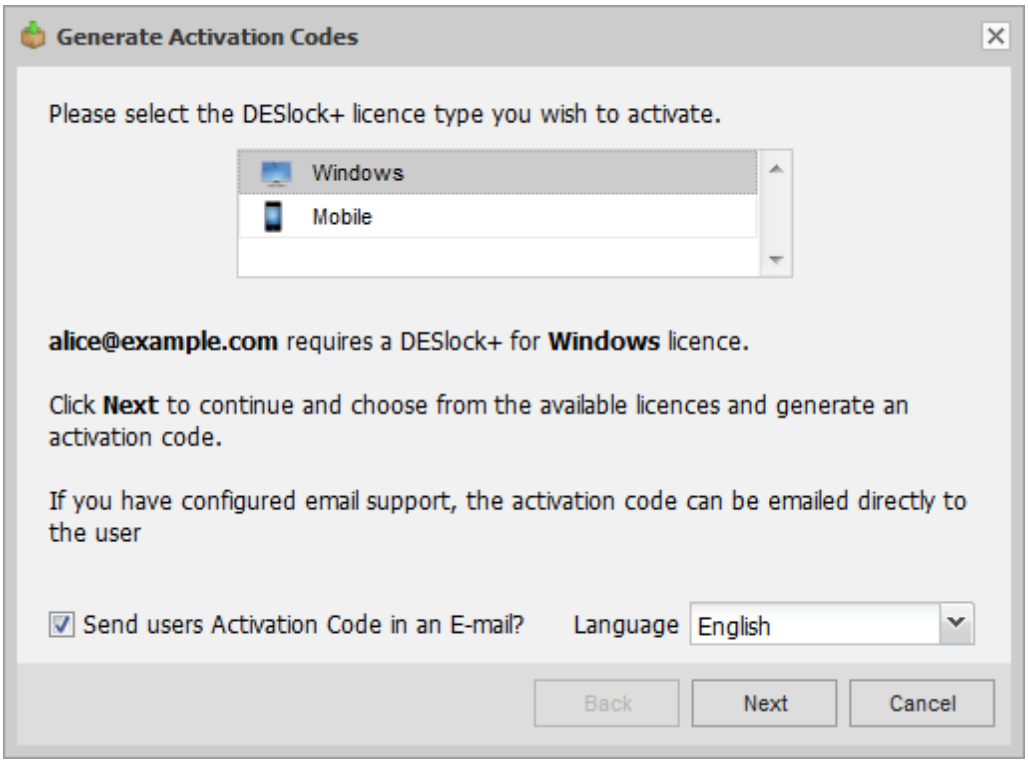
To issue a licence to a user, you need to send them an activation code.

To do this, select the user's team in the Navigation panel, then select the 'Users' tab. Highlight the user that requires a licence (this can be easily seen by the display colour of the user – unlicensed users appear as grey) and click the "Generate Activation Codes" button.Multiple users can be selected and issued a licence simultaneously by holding down shift and clicking the required users and then by clicking the "Generate Activation Codes" button.

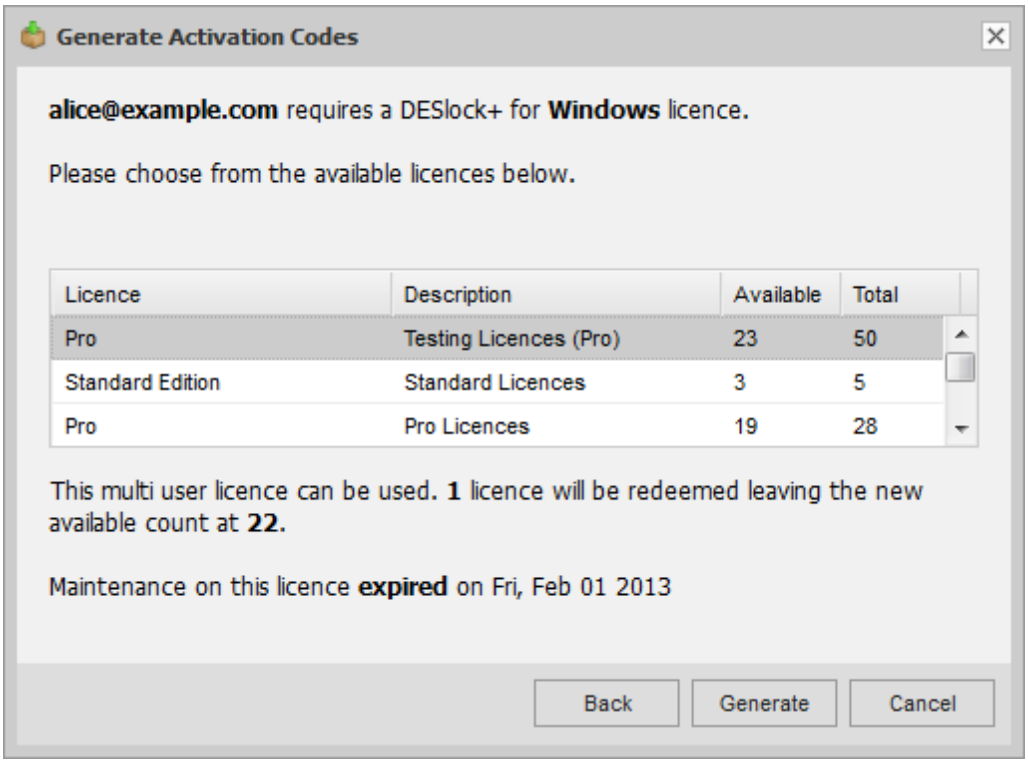


You must firstly select the type of licence you wish to generate. The list of available types is based upon the types of multi-user licences you have currently added to the Enterprise Server. If you want to send the code to the user by email, leave the 'Send user their Activation code in an email' check box checked. You may also choose a different language for the email, if you have multiple language templates installed. Sending of the

email is optional at this stage and you can resend the email at a later date if required.



If the user requires a licence of the selected type, you must next select which specific multi-user licence to use. Click 'Generate' to generate an activation code. The user's state will change from grey (no licence) to blue (not active).



If required, at a later time but before the user has activated, you need to issue the activation codes to the user, select the user, click the 'User Details' button and then in the User Details window select the 'Activation Codes' tab. To send the email again click the 'Send Email' option.

User Activates their Workstation

The next stage is for the user to activate their workstation once the software installation has completed. For details see Workstation Activation

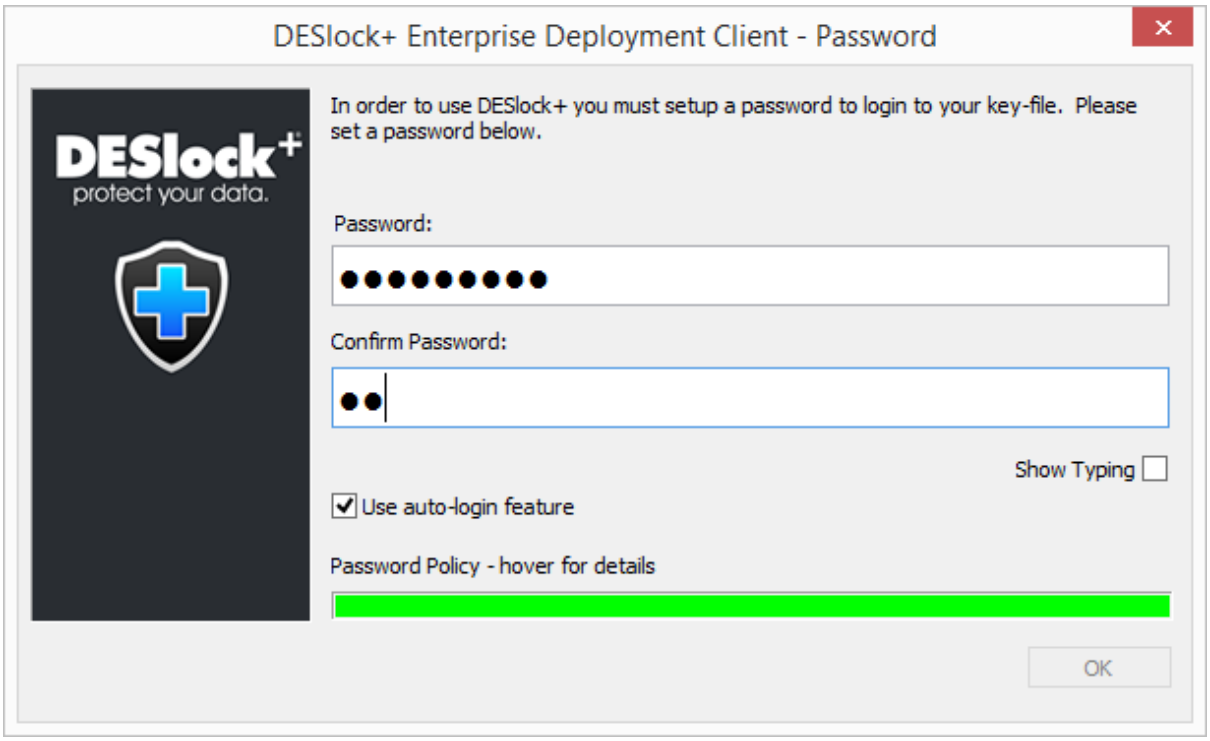
11.3 Workstation Activation

The user will have the DESlock+ Activation window showing each time they use their computer until activation is performed. To complete the installation the user will need to enter the activation code sent by the system administrator.

Enter the code and click 'OK'. The system will validate itself with the Enterprise Server (via any proxy's) and update the group policies and Key-File for that user.

User Password

Post activation, the first action the user has to do is set their password. This is controlled by the group policy for the user's team, so may require the use of upper case, lower case, numbers, symbols or be of a minimum character length. If the user hovers over the “strength meter” they will see the policy settings currently set for this password. Once a password which conforms to the password policy has been typed the status bar will change to green. The 'OK' button will be greyed out until the password has been confirmed and matches the initially input password. To verify any errors check the 'Show Typing' box.



If the workstation policy "Allow Key file Auto Login" is enabled for that workstation, the user can check an additional box "use Auto-login feature" which will use the Windows login as authority to start DESlock+. If this feature is not available or selected the user will have to log in to DESlock+ as described below. To log out right click on the DESlock in the Notifcation Area (also known as the System Tray) and select 'Logout' or double click on the icon.

Periodically, depending on parameters set within the policies defined by the system administrators, the client workstation will synchronise with the Enterprise Server. This allows updates and changes to be sent by the administrator and
implemented on the workstation. For details see Synchronisation.

DESlock+ logged in

DESlock+ logged out

Next time the user starts their PC they can log into DESlock+ by right-clicking the DESlock in the Notifcation Area (also known as the System Tray) and select 'Login' or the user can double click on the icon. Windows 7 Users please refer to the note at the end of the section.

Then enter the password they provided during registration.

Once the user has logged into DESlock+ they can use the encryption features permitted by their administrator.

In this instance, where a new user has been activated on a new workstation, the workstation and Enterprise Server will need to be synchronised before the user and workstation will appear as normal (green) in the

Enterprise Server.

Windows 7, important note

With Windows 7, any new Notification Area icons (also know as System Tray) icons (such as DESlock+) are hidden shortly after being installed. To view any hidden icons simply click the up arrow next to the other system tray icons and clock. If required the DESlock+ icon can be moved (dragged) into the main system tray, or using the customise feature (click the system tray up arrow, then select customise) its default position can be changed.

11.4 Synchronisation

To ensure that both the Enterprise Server and the client workstation are up to date, the system periodically checks for any updates (synchronises). The Enterprise Server updates every 30 minutes and the workstations every 60 minutes. (This is a default setting - the workstation setting can be changed within Workstation Policies.)

At any time both the administrator and the client can force a synchronisation. Synchronisation provides the method by which updates and changes are sent by the administrator and implemented on the workstation.

Normal Status

The "normal" status of both users and Workstations is green, any other colour means that some action is required to be completed.

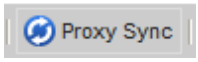
For example when a new user is created they will appear grey until they have a licence issued to them. They will then appear as blue until they are activated on a workstation (either an existing or new workstation). At that point they will only appear green when both the Enterprise Server and the workstation have synchronised.

Once both the user and the workstation have appeared (this is dependent on the workstation policy “Background Update Check Period”), updates and changes can be made.

Manual Synchronisation

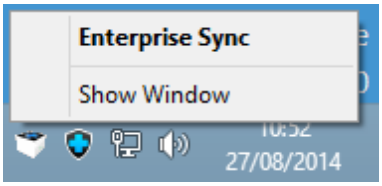
Enterprise Server

If the workstation does not appear, the administrator can force a synchronisation by clicking the 'Proxy Sync' button at the bottom left of the browser window.



Workstation

It may also be necessary for the user to synchronise from the workstation. To do this the user needs to right click on the Enterprise Server icon in their Notification Area (also known as the System Tray) (box symbol below), then select 'Enterprise Sync'.



It is also possible for the user to view system messages from this control too by right clicking on the Enterprise Server icon, selecting 'Show Window' and then the window below will display all messages

between the Enterprise Server and their workstation. Click on the 'More >>' control to show additional information.

Additional details are shown as below. You can also select the 'Sync' button to sync with the Enterprise Server from this window as well.

Once the Enterprise Server and the workstation concerned are both in sync, the workstation and the user will appear as green. The only status that is different is where the user has been supplied with different keys from the rest of the users in their group. In this case they will appear as purple. See Interface and Main controls for details on the user status colours.

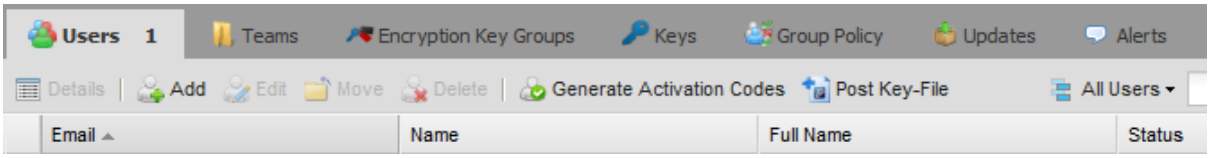
11.5 Updates

Once both the workstation and client are active, any changes to the user details (key groups added, policy changed) and the status of the user(s) will alter (colour change) and they will require a new Key-File to be supplied by the administrator. Similarly, if workstation policy is changed the workstation will change colour to indicate it requires a policy upfdate.

The user will require an updated Key-File to be posted (which contains keys and policy) by the administrator. Next time the user logs in, DESlock+ will automatically implement the policy settings for that user. The workstation will require a policy update which should be applied by posing a policy update.

In the example below users Alice, Charlie, Dave, Eddy and Fred are red and require updates (in this case changes were made to the group policy settings). Gavin and Henry were created and activated after the changes were made and so are green.

To update these five users, select them (ctrl click), then click 'Post Key-File'.



Once posted and the background task has completed, each user's status colour will change to orange (update pending).

When the client (user) next logs on the change will be implemented automatically, unless the administrator has allowed the user to postpone any updates by checking the relevant check box in the Enterprise Server.

Once both the Enterprise Server and workstation have synchronised, the user's status will change to green (normal) unless the user has additional keys, in which case they will appear as purple. If required, both the client and the administrator can synchronise manually as described in Synchronisation.

12 Adding a Mobile Device

The process of adding a Mobile Device is similar to adding a normal workstation.

Currently only only iOS is supported. Firstly you need to download and install the DESlock+ iOS app from the Apple App Store:
https://itunes.apple.com/us/app/deslock+-for-ios/id880602467?ls=1&mt=8

See next:
DESlock+ for iOS

Managing in Enterprise Server

12.1 DESlock+ for iOS

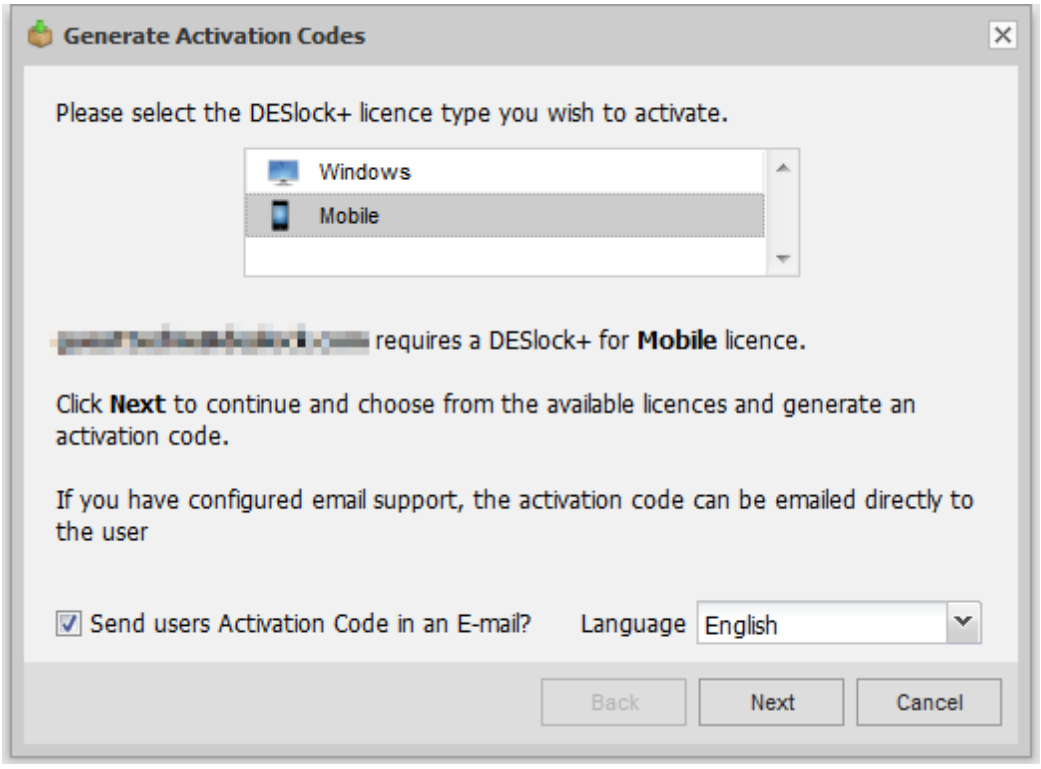
DESlock+ for iOS App

After installation you should have the DESlock+ for iOS app installed. Until it has been activated the DESlock+ for iOS app will function only in free mode.

DESlock+

Generate Activation Code

From within the Enterprise Server you generate an activation code as normal. Select the Mobile licence type. Please note that you must have added a Mobile licence type to your Enterprise Server for this to appear.

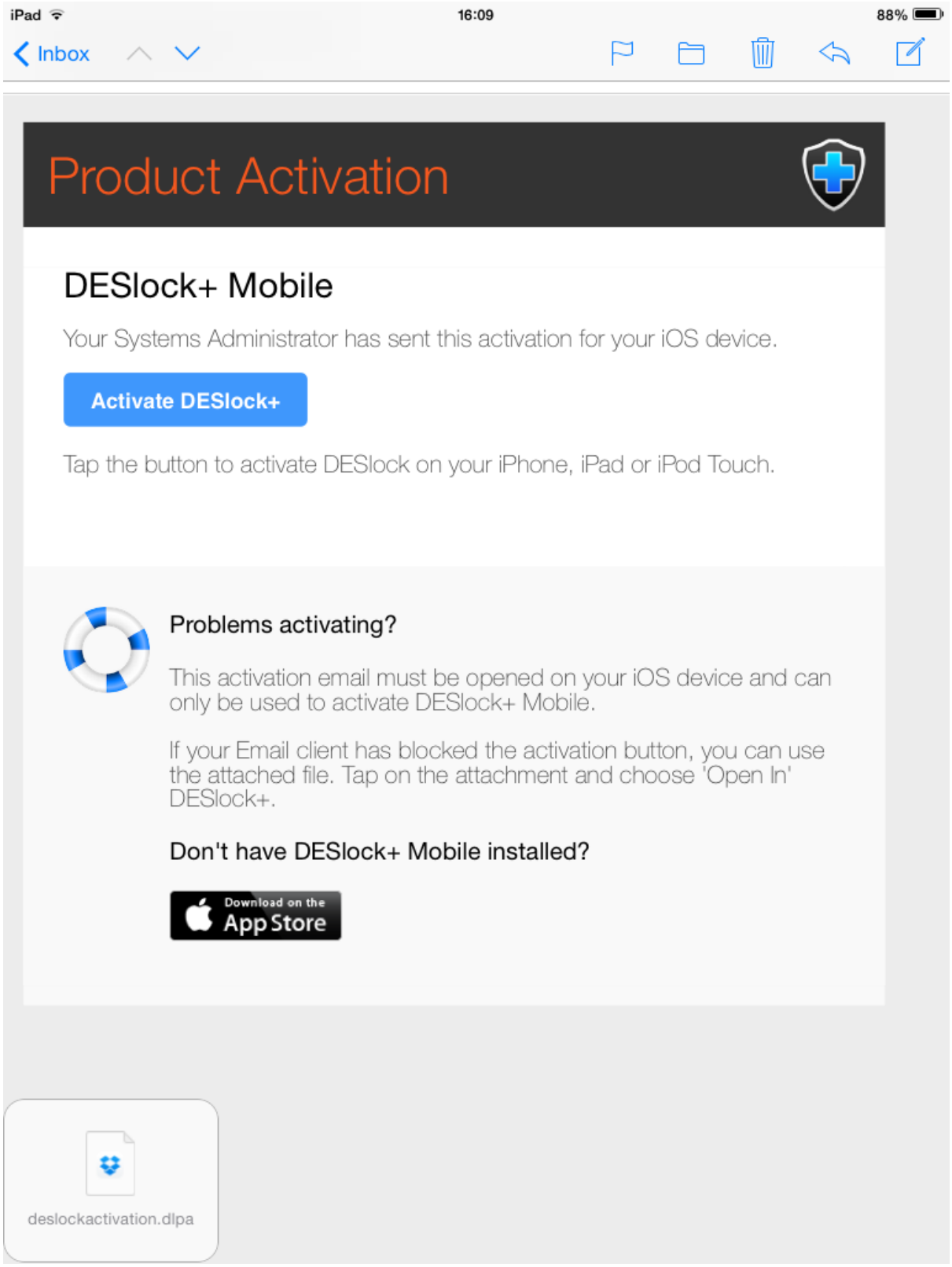


Please note that sending of the email is required. The user must have a valid email address to which you can send the activation email.

Apply Activation Code

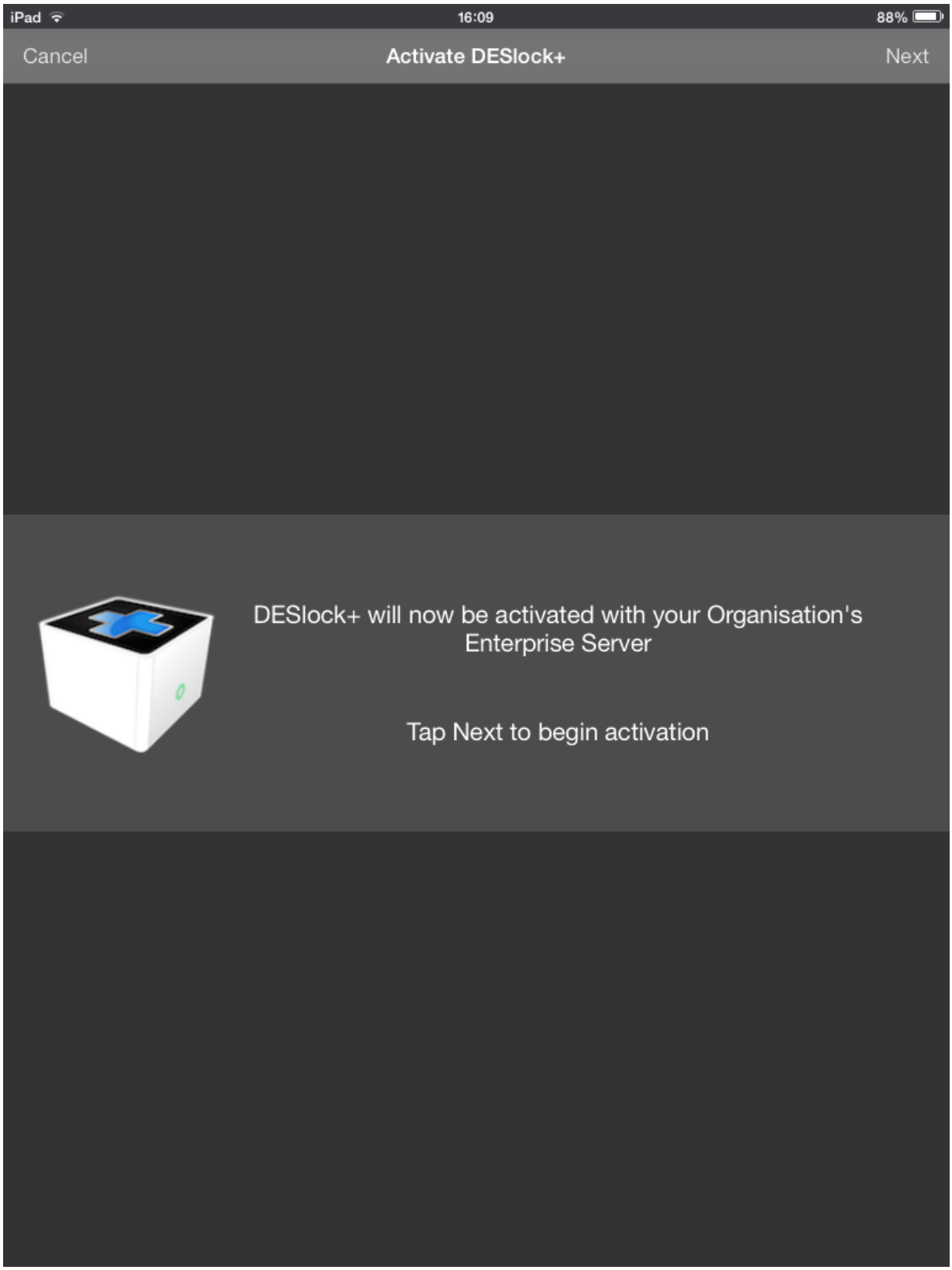
On the mobile device the user will receive an activation email. Simply follow the instructions in the email and

click the Activate button. If the activation button does not work for some reason, you should open the attachment with the DESlock+ App.



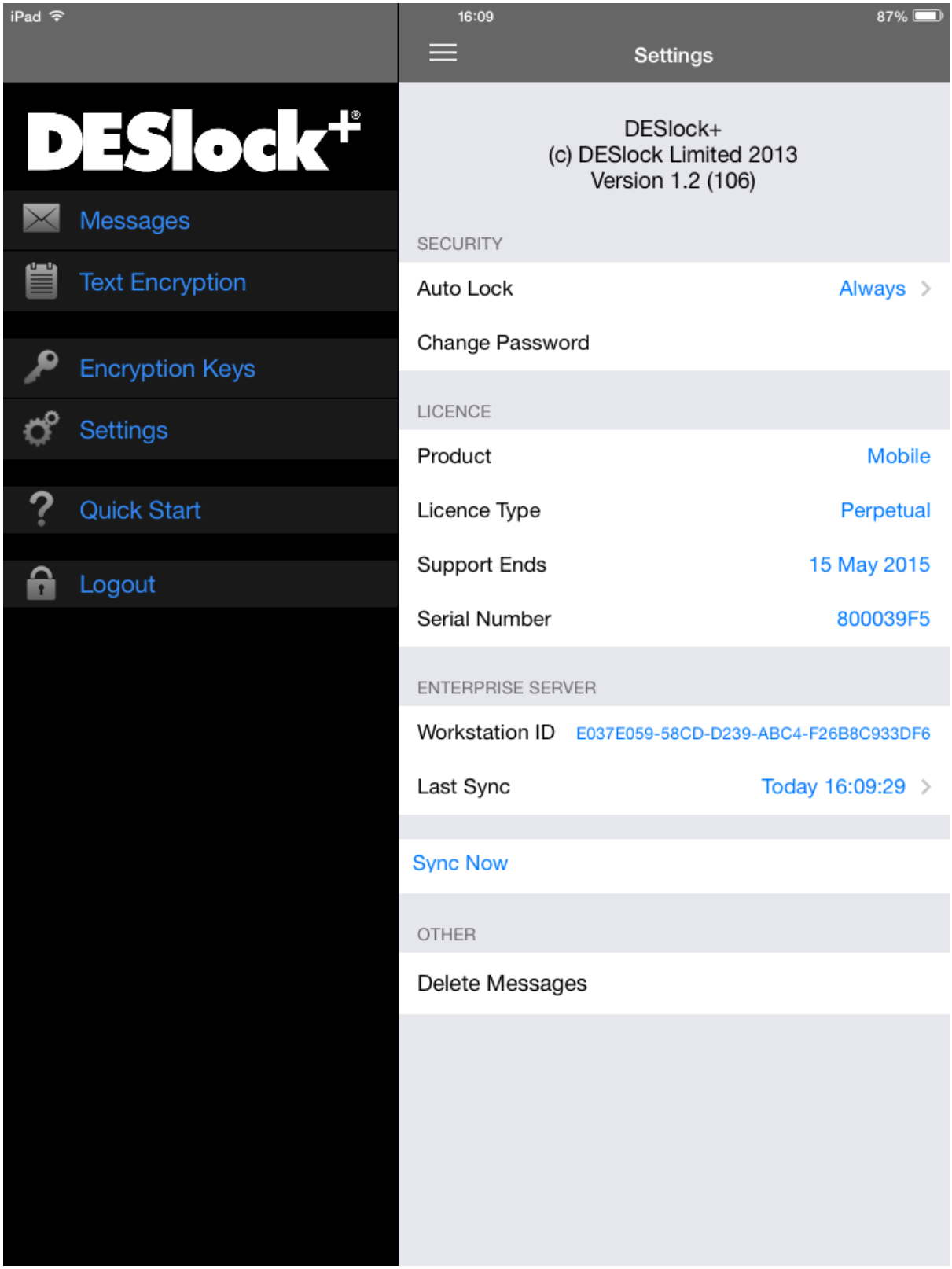
Activation Process

Once you have initiated the activation process, the iOS App will launch and will prompt the user to choose a password for their Key-File.



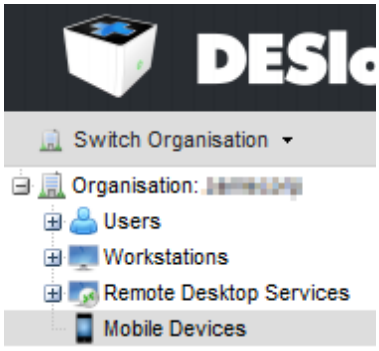
Complete this process and choose and confirm the password and any other settings as prompted.

Once the activation process has been completed, the DESlock+ for iOS app will display activated status along with details of the licence, and allows access to the encryption keys.

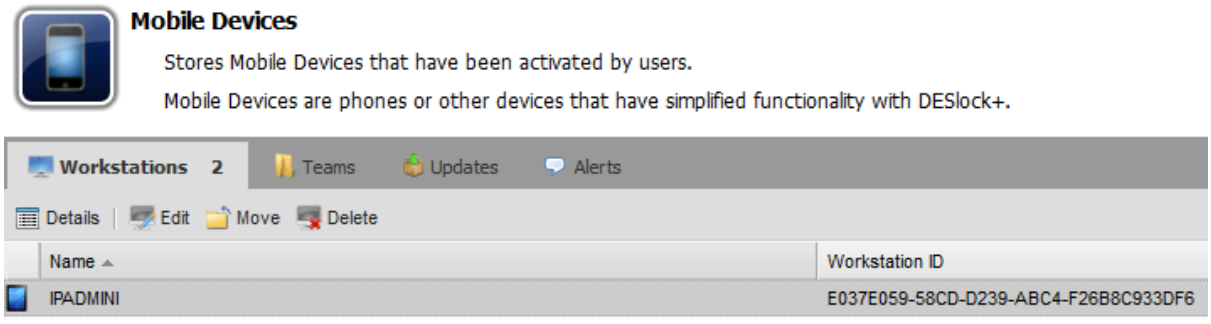


12.2 Managing in Enterprise Server

Once at least one mobile device has been activated, they will be added to the Enterprise Server to a special Team called Mobile Devices.



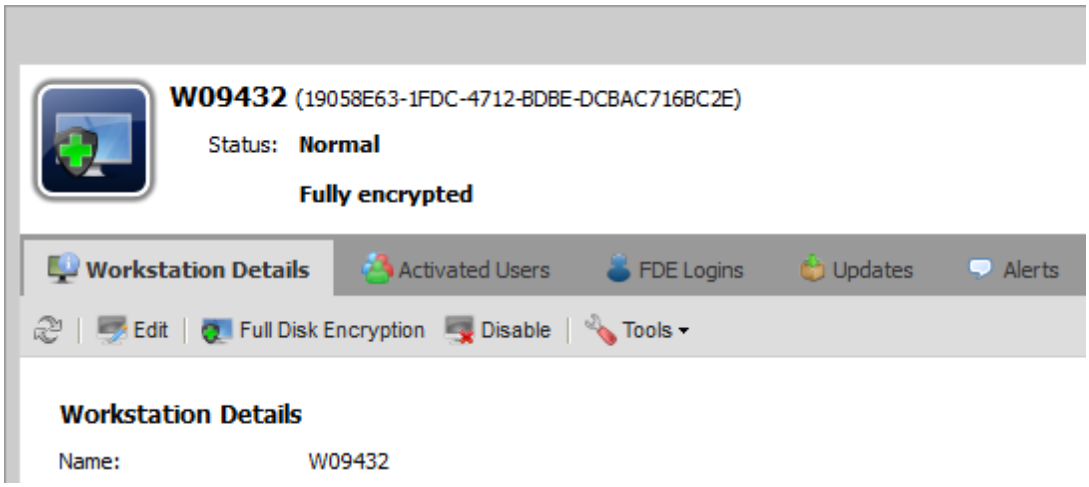
Mobile Devices are different from normal workstations in that they currently do not have workstation policy applied to them. Nor can you currently send any Full Disk Encryption commands to them. However other aspects are the same and from the Mobile Devices view you can see the status of any posted Updates and view any Alerts that relate to these devices. You can also create sub teams for the purposes of organisation if you wish.



13 Full Disk Encryption

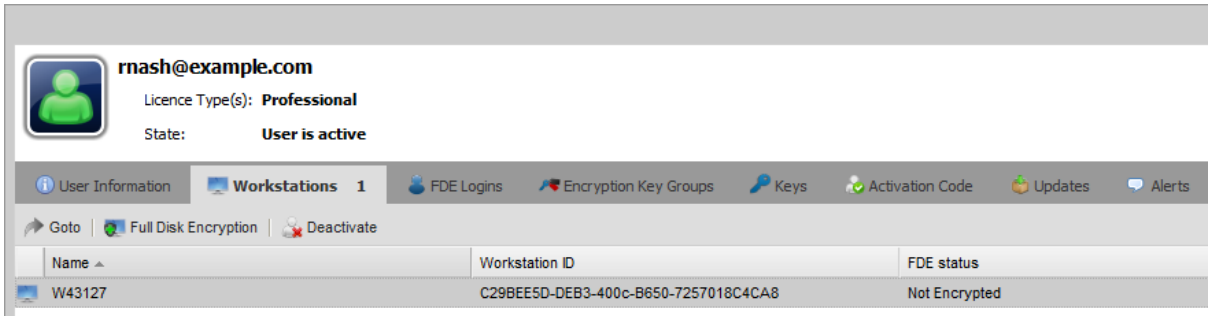
With an activated user and workstation displayed in the Enterprise Server, the administrator can remotely initiate full disk encryption on that machine.

You can do this on one of two ways. Firstly select the 'Workstations' tab, and highlight the workstation. Click the 'Details' button (or double click the workstation). Click the Full Disk Encryption button.

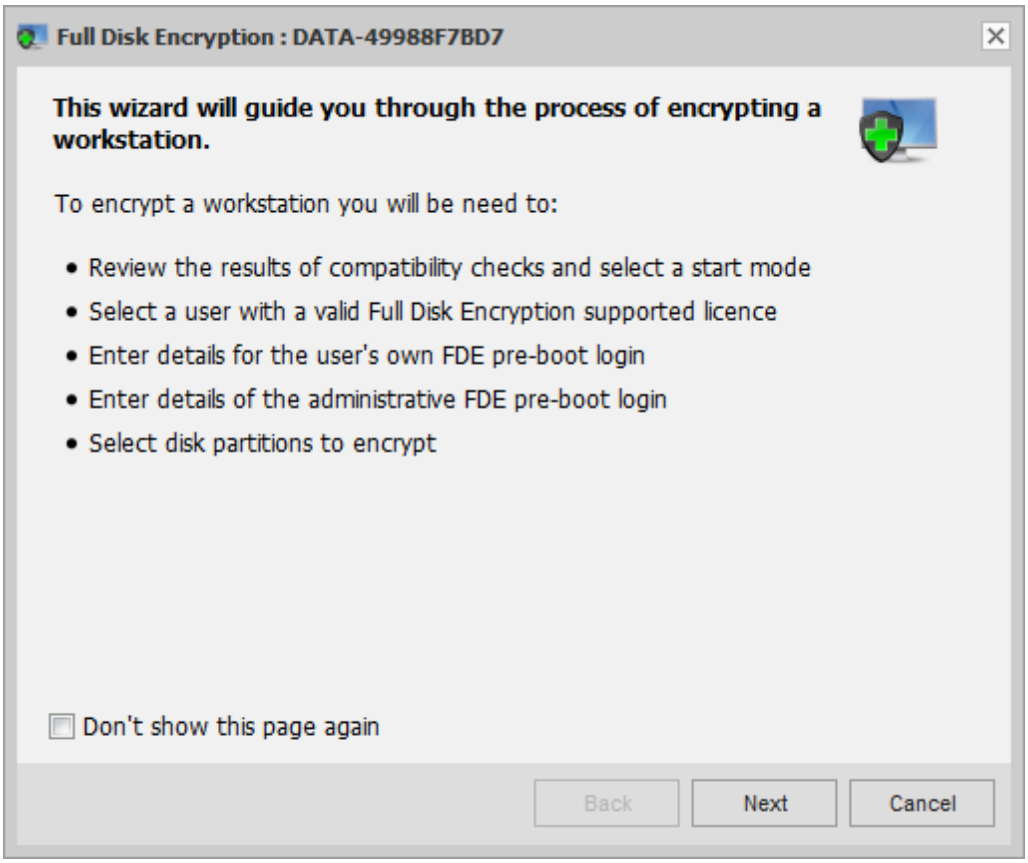


The second method is to select the 'Users' tab, highlight the user whose workstation is to be encrypted and click the 'Details' button (or double click the user).

In the user's 'Detail' sub window, select the workstation tab then the user (Henry) and click the 'Full Disk Encryption' button.



The Full Disk Encryption wizard will show, as below.



- Compatibility Checks

This checks the workstation information for any known incompatibilities. Depending what is found, you may choose to start encryption normally; start encrypting in safe mode; or override the safety checks and force encryption to start.

  - Normal
  - Safe Start
  - Bypass Safety Checks

- Select User

If the Encrypt Wizard was started from a Workstation card, without a user context, you must select the user in this wizard. If you start the wizard from the User card, this page is skipped as the user choice is implicit.

- FDE Login Details
  - Username - this does not have to be the username as shown, it can be a generic name for the workstation
  - Password - either define a password or use the system generated one.
  - Password attempts - define the number of password retries permitted.
  - Recovery password uses - define the number of times a single recovery password can be used
  - Email FDE Login details - Select whether to send the user their FDE login details by email
  - Single Sign-On (SSO)
    - User must confirm password - the user must provide a valid password (as defined by the administrator) before encryption commences. If this option is selected the number of system starts permitted without initiating full disk encryption must be defined. Once that number is exceeded the encryption process will commence.
    - User can choose password - users can define their own password before the process will start.
    - User can change password - allows the user to change their FDE password.

If you opt to change Administrator FDE Details

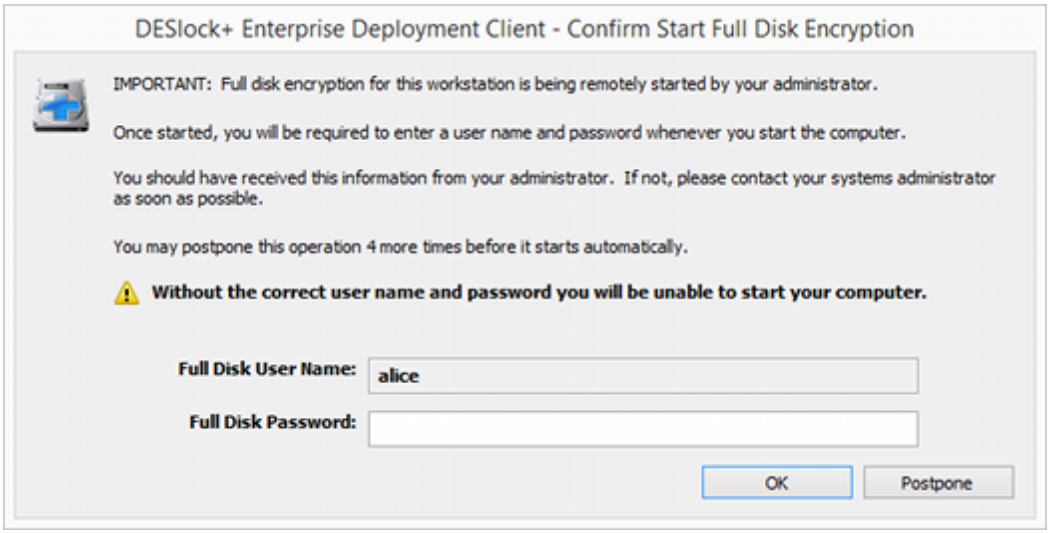
- Admin Login
  - Admin name - enter the admin name for the workstation.
  - Password - the password is not the Enterprise Server administrator login password, this is unique to the full disk encryption process and is controlled by password policy settings, so may require the use of upper and/or lower case letters, numbers and minimum password length.
  - Password retries (if selected by check box) - enter the number of admin password retries permitted before the workstation is locked.

If the workstation has reported sufficient data to allow a disk selection
- Select disk partitions to encrypt

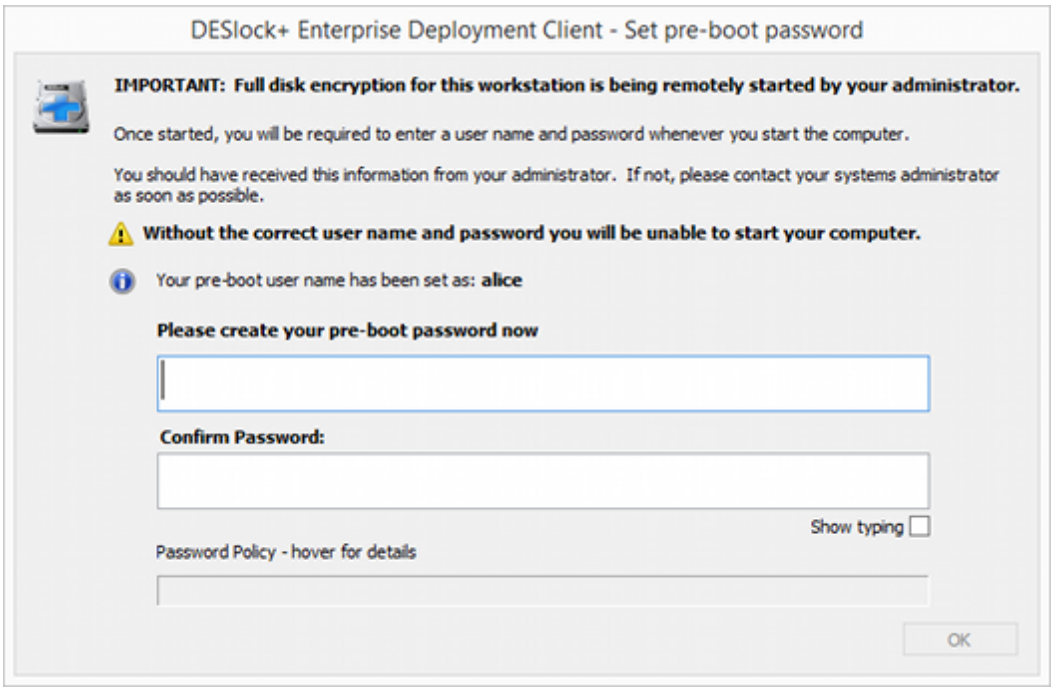
Once all options have been selected, a summary will be shown. Click 'Encrypt' and the Enterprise Server will start the process on the workstation.

The workstation user will see the following messages (dependent on the options selected).

User must confirm password. If the administrator has selected this box during encryption initiation, the user will see the following before encryption starts - If this box was not checked the encryption will start without warning. Note that in the instance below the user is allowed 5 system restarts before encryption will be forced on their machine.



User Can choose initial password. If this box has been selected, the user will see the normal password definition window, as below. As before, password policy is enforced and the hover clue is available.

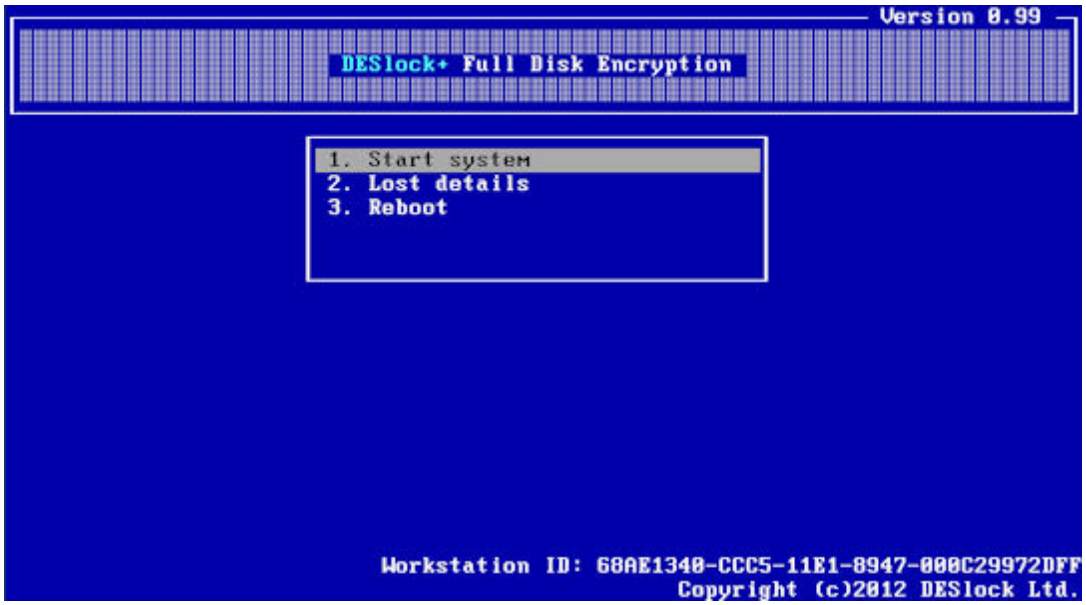


Once the password has been correctly entered twice, the full disk encryption process will commence and a status windows will show.

The user's machine can be used as normal during the encryption process and can be powered off if required with encryption continuing from the point it had reached when the machine is next used. Note, disk encryption will not restart immediately when the machine is switched on, a period of five minutes is set for all system processes to stabilise before encryption is resumed.

The Enterprise Server will also show the encryption status, although it is only updated when the workstation and Enterprise Server are periodically Synced.

Once the encryption process is completed the machine will be restarted and the user will see the following screen during initial boot up. To start the machine normally select option 1 (the mouse wont work, they have to use the keyboard arrows or select a number) and press return. The user then needs to enter their username and password. The system will then start. Depending on policy settings, they may then no longer need to enter a password to use DESlock+ to locally encrypt data using specific keys.



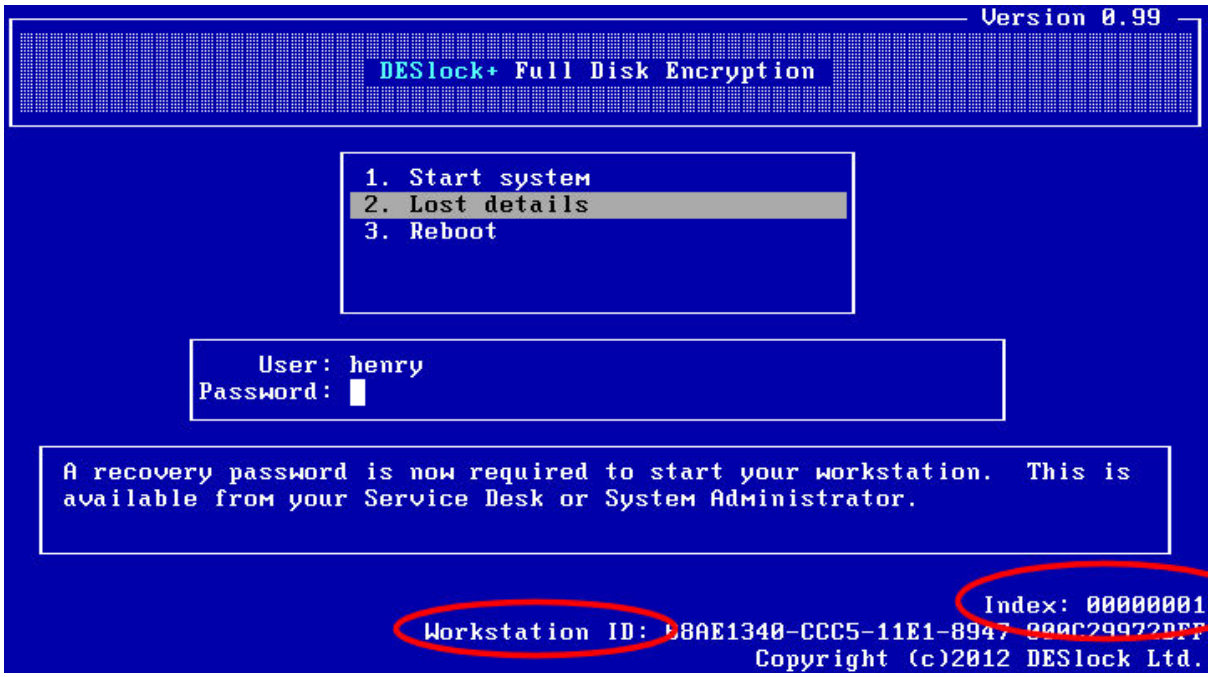
The Enterprise Server will also report that the encryption has completed and will display the current status of the user and workstation as below. Note that the user and workstation both are green.

13.1 Lost Details

User Workstation

If a user forgets their full disk encryption password, they should select the 'Lost details' option at the login screen. They should then:

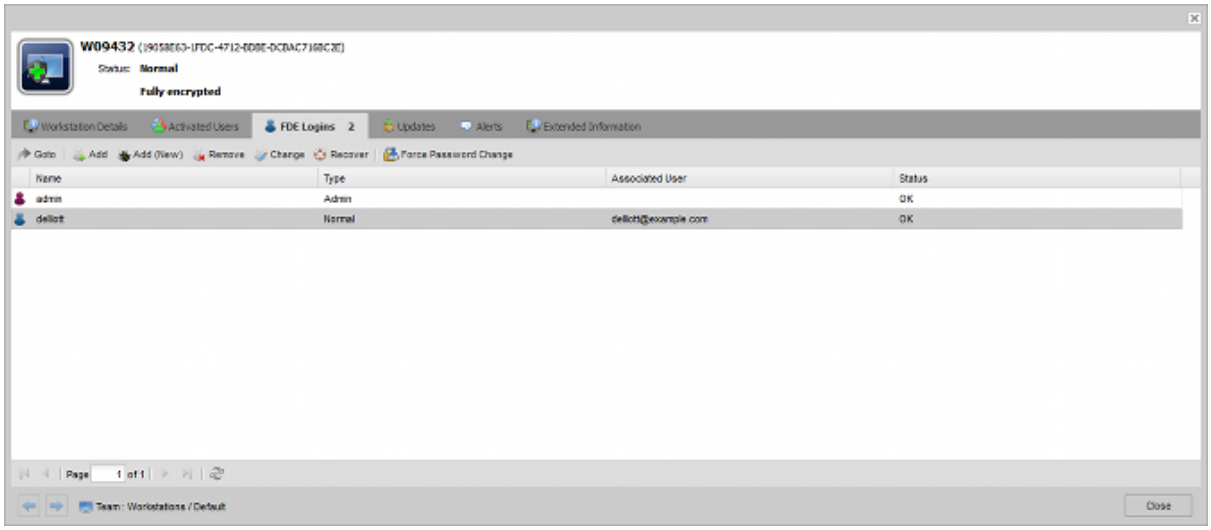
- Enter their username and press return.
- Note the Index number and workstation ID (circled below in red)
- Report the username, Index No. and machine details to their network administrator.



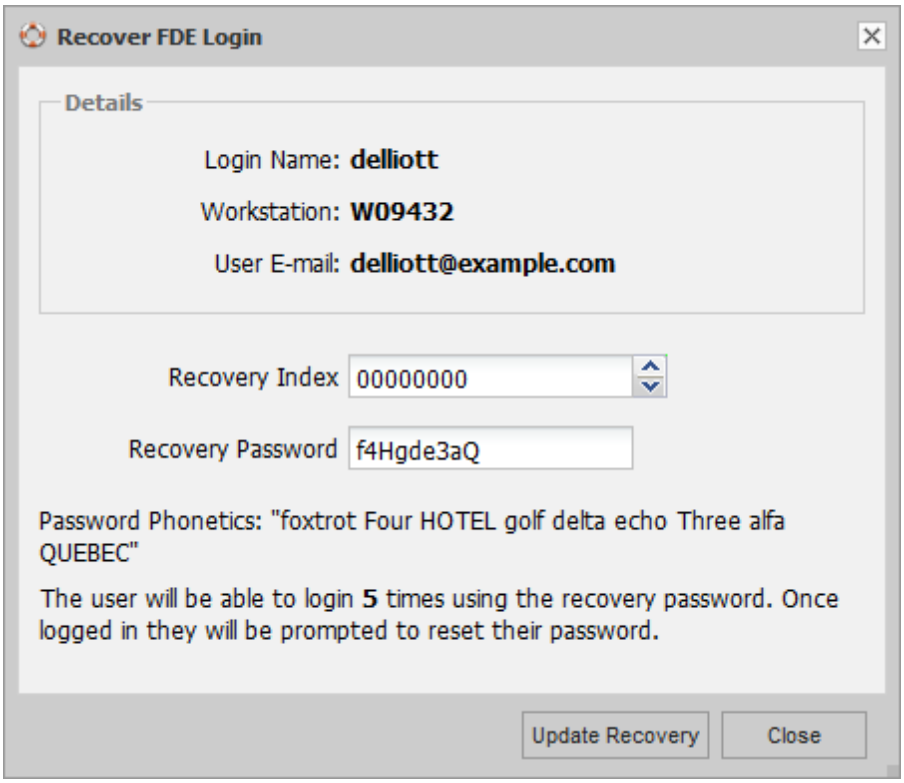
Enterprise Server Administrator

To recover the user the administrator should select the correct team in the Navigation panel, then the 'Workstations' tab and highlight the user concerned, then click 'Details'.

In the details panel, select the 'FDE Logins' tab and the affected user, then click 'Recover'.



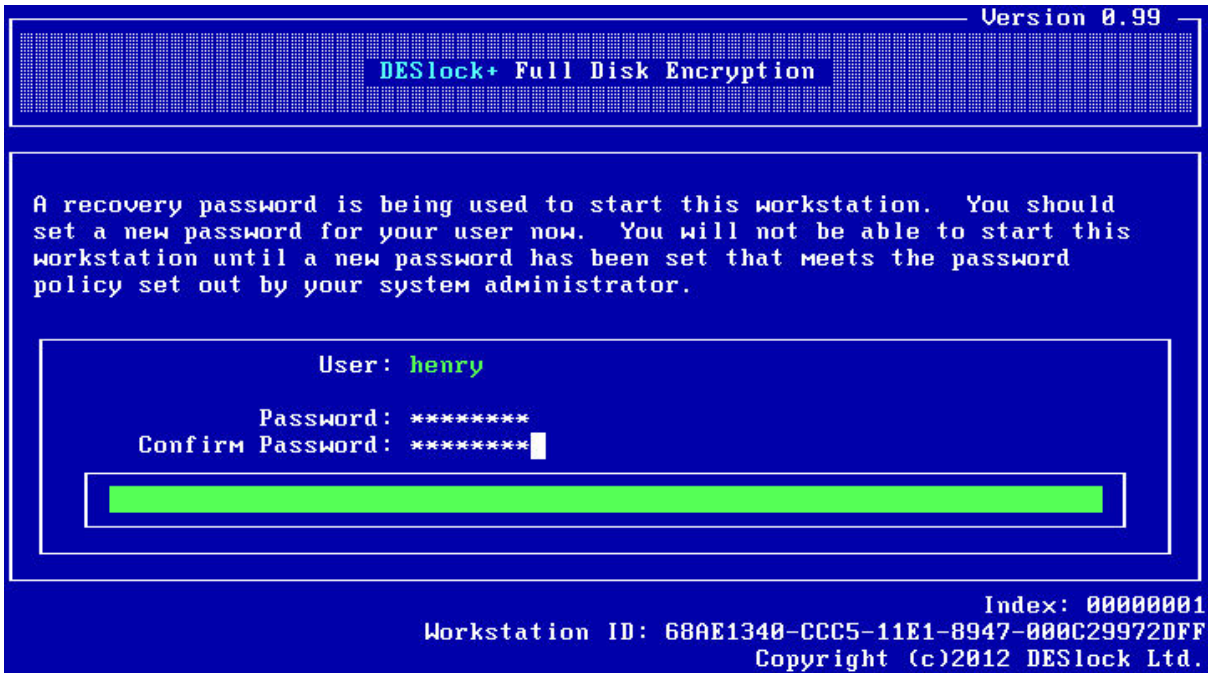
If there are many workstations in use, it may be simpler to select the team in the Navigation panel, then select the 'Users' tab and highlight the user concerned. Click the user's 'Detail' button, then in the sub window select the 'FDE Logins' tab. Highlight the FDE user login, then click 'Recover'. By either route the recovery window will show next.



Make sure the Login Name, Workstation and Recovery Index matches, then supply the user with the Recovery Password.

User Workstation

The user has to enter the password exactly as supplied (upper and lower case, and numerics) in the screen as shown at the start of this section (above) and then press the return key (enter). In the next screen they will then have to redefine their own password, following the normal policy settings for password strength (shown by the status bar).



Once their new password is defined, the system will start as normal.

Enterprise Server Administrator

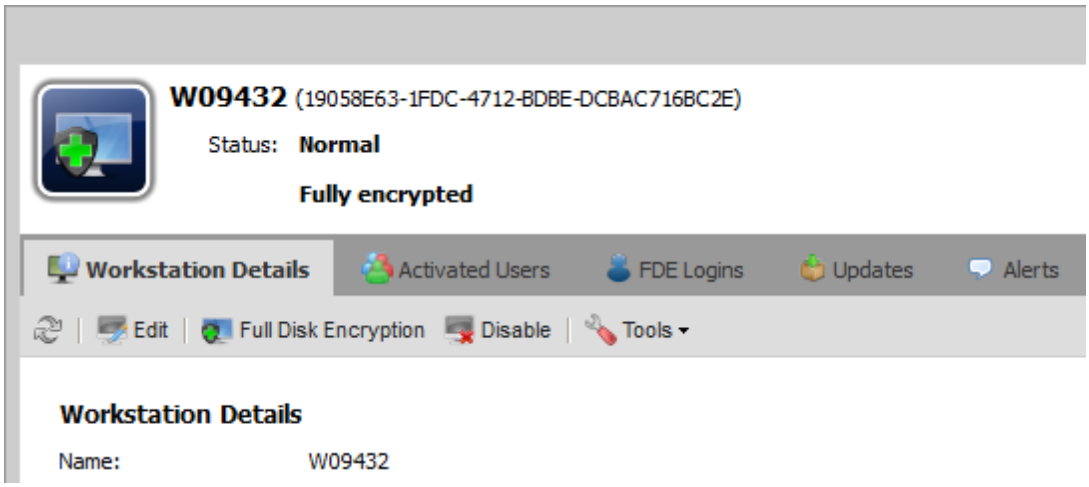
The administrator will need to reset the recovery index, once the user has logged into windows.This is performed in the "Recover FDE window", as shown above. The administrator clicks the 'Update Recovery' button. This increases the Index by one, and prevents any further use of the first recovery password.

13.2 Disabling Workstations

Disabling a workstation may be performed as follows. In the Navigation panel select the team, then on the menu bar select 'Workstations'. Highlight the workstation (Henry, in the example below) and click on details.

Important. Once a user's full disk encryption login has been removed it cannot be re-instated. There are two ways a workstation may be disabled, either a normal workstation user login can be removed or all full disk encryption logins can be removed. If only the user login is removed, the data on the HDD can still be accessed by the admin user. If all users are removed, all data on the HDD will remain encrypted and secure. In this case the HDD will have to be reformatted and a new OS installed before the drive may be used. All data will be lost.

In the details panel click on 'Disable'



Select the type of disable required.

- Remove only user FDE Logins - this will remove the FDE logins from authorised users (except the admin user).
- Remove all FDE logins - will remove all FDE logins, including the admin user. The HDD will no longer be accessible and will remain encrypted.

You may optionally also choose to reboot the workstation once the command has been processed. This will cause the workstation to **immediately** reboot. The user will **not be** given a chance to delay this reboot, **nor will they be** prompted to save any files which may be open!

Note: if you choose to remove all FDE logins, you will be required to input your administrator password.

You will be prompted to enter your administrator password (if ALL FDE logins are being removed) before the task can be completed. If only user FDE logins are being removed this will take place immediately.

The disable command will be sent to the workstation and will take effect at the next login after the Enterprise Server has next synchronised with the server proxy. From that point on the workstation will no longer accept passwords for the user. The HDD will be available to the admin user.

If the second option has been selected, the workstation will not accept passwords for any user.The HDD will remain encrypted and inaccessible. Only a complete format and re-installation of the OS will recover the machine, but all data will be lost.

DESlock+

protect your data.