

Enterprise Password Safe

Manual for EPS version 1.58

©Copyright 2003-2008 Enterprise Data Safe Limited, All Rights Reserved.
Redistribution, Installation, Reverse Engineering, or Use of the application without an
appropriate license is forbidden by law.

Contents

Introduction.....	3
Licensing.....	3
Configuration matrices.....	4
Installation.....	5
Default user details.....	5
Page Layout.....	6
The password hierarchy.....	7
Editing the password hierarchy.....	7
Importing data from files.....	8
Password creation.....	9
Password deletion.....	9
Password modification.....	9
Password restrictions.....	9
Edit password access controls.....	9
Personal Password Folder.....	9
Outstanding Restricted Access Requests.....	9
User creation.....	10
User deletion.....	10
User modification.....	10
User authentication.....	10
Group creation.....	11
Group deletion.....	11
Group modification.....	11
Audit logs.....	12
Audit alerts.....	12
Appearance.....	13
Configuration options.....	13
Database configuration.....	15
Systems details.....	15
Integration modules.....	15
Network zones.....	15
All passwords report.....	16
User access report.....	16
Tips.....	17
Appendix A - Developing integration modules.....	18
Appendix B – External API.....	19
Common Parameters.....	19

Introduction

The Enterprise Password Safe provides a centralised password repository and maintains an audit trail of accesses to the stored passwords. The EPS has numerous security enhancing features such as;

- Restricted Access Passwords which require other users to approve access to passwords
- The EPS encryption chain which ensures that passwords are not accessible without breaking at least one of the currently established encryption standards.
- All password data encryption is performed in application memory to avoid data being transmitted or stored in an unencrypted form.
- SMTP Email alerts sent to administrators when passwords are accessed.

We value feedback from all users and make use of the feedback to develop the product to ensure you are able to use our software to meet your needs. If you have an idea or suggestion for improving the Enterprise Password Safe please send a message to us via the contact form at <http://www.enterprise-password-safe.com/contact.html>

Licensing

You will need a license before you can create passwords, users, or groups in the EPS. You can log into the system without a license, but attempts to perform some of the functionality of the EPS will result in an error being displayed. To enter a license key you should select the *License* option in the system menu on the left of the screen and paste your license code into the box provided. Once the license has been accepted your license details should be displayed.

You may use the EPS under the following conditions;

1. The Enterprise Password Safe must not be disassembled, reverse engineered, or modified in any way without the written consent of Enterprise Data Safe Limited.
2. The Enterprise Password Safe must not be operated without a valid license issued by Enterprise Data Safe Limited or one of it's approved resellers.

Any single breach of these conditions will be taken as an agreement by the party committing the breach to pay Enterprise Data Safe Limited one million Euros as compensation. If these conditions are breached on multiple occasions the party committing the breach agrees to pay one million Euros for each calendar day these terms were breach on.

Enterprise Data Safe Limited does not accept financial liability for any consequences resulting from the use this program.

If you have problems with your license, or wish to obtain a trial license please contact us via the contact form at <http://www.enterprise-password-safe.com/contact.html>

Configuration matrices

To assist with the creation of users and the correct assignment of accessing and viewing rights we recommend using a spreadsheet which has the following three parts;

1. A User List – This list contains all of the people who will be using the EPS.
2. A Group List – This list contains all of the groups that will be created in the EPS and the users from section 1 who belong to the group.
3. A Password list – This list contains all of the passwords which will be managed by the EPS, a list of which groups have read only access, which groups have modification access, which users have read only access outside of the groups they belong to, and which users have modification access outside of the groups they belong to.

The lists would look similar to the ones below;

Users

User name
alice
bob
charlie

Groups

Group name	Members
Unix Admins	alice, bob
Tech. Services	charlie

Passwords

Password	Groups (read only)	Groups (modify)	Users (read only)	Users (modify)
“root” on unix01		Unix Admins		
“nagios” on unix01	Tech Services	Unix Admins		
“root” on nfs01	Unix Admins			bob

This would give alice and bob the ability to modify the password entry for the users “root” and “nagios” on unix01. Alice would be able to read the root password for “root” on nfs01, and bob would be able to modify it, and charlie would be able to read the password for “nagios” on unix01, but not modify it.

Installation

There are three methods of installing the EPS;

1) Executable Installer

These are available for Windows and Linux on Intel/AMD x86 and Solaris on Sparc, these will take you through the steps necessary to install and configure the EPS.

2) Compressed Installations

These are archive files in ZIP and Tar with GNU Zip formats which contain all the files necessary to run the EPS. To use these you must install a Java Virtual Machine compatible with Java 5 or above.

3) WAR file for application servers

If you are running your own Java Application Server you can deploy the EPS to it and run the EPS from within it. To use the EPS war file your application server must support Java 5 or above, the Java Servlet specification version 2.4 and above, and Java Server Pages (JSPs) version 1.2 and above.

If you are using either the executable installer or the files extracted from a compressed installation and you want to use a supported external database you should do the following;

- 1) Download the appropriate Type 4 JDBC driver from your database vendor.
- 2) Ensure the EPS is not running.
- 3) Copy the driver files into the lib directory within the jetty directory inside your EPS installation directory.
- 4) Start the EPS.

You should then configure the connection to the database from the Database option available on the left hand menu when you log in as an administrator.

If you choose to use an alternative application server you should consult your application server vendor for instructions on how to install JDBC drivers.

You can find further information about installing, configuring, and operating the EPS in the online FAQ at <http://www.enterprise-password-safe.com/support-faq.html>

Default user details

After installation the only user available has the user name *admin* and the password *admin*.

We recommend that you change the password for this user as soon as you log into the system.

Page Layout

All EPS pages have the same design, an example of which is shown below;

The screenshot shows the 'EPS : Password Hierarchy' page. At the top right, it displays 'Your account : admin | Change Password | Logout'. Below this is a dark blue header with the page title 'EPS : Password Hierarchy'. On the left is a vertical navigation menu with sections: Passwords (View/Edit, Search, Expiring, Personal, Create, Import, RA Requests, Restrictions), Users (View/Edit, Create, Delete, Import, Authentication), Groups (View/Edit, Create, Delete, Import), Events (View, Settings), System (Configuration, Custom Fields, Database, Details, Integration, Network, Zones, License), and Reports (All Passwords, User Access). The main content area has a search bar with 'Username' and 'System' fields and 'Search' buttons. It shows 'Currently viewing : Top Level' with a link to 'Click here to edit the hierarchy'. Below the search bar, there are two sections: 'Sub-Folders' and 'Passwords', both displaying 'None'. A note at the bottom of the 'Passwords' section says 'Sort by username or system , ! = expired password.'

There are four main areas to any EPS page;

- 1) The account bar at the top of the page which contains information and options relating to the user currently logged in.
- 2) The page title shown in the area with the dark blue background below the account bar.
- 3) The action menu of the left of the page showing the actions available to the user
- 4) The main area where the information is shown.

The options on the action menu will change depending on type of user logged in. The example above shows all of the options available to a full administrator.

The password hierarchy

The password hierarchy allows passwords to be categorised into folders, and each folder may contain passwords and sub-folders which contain further folders and passwords without limit. The hierarchy can be viewed by clicking on the *View/Edit* option under the *Passwords* heading from the menu.

The password hierarchy has a separate set of permissions which allow administrators to control access to passwords based on their location in the hierarchy. The hierarchy permissions take precedence over individual permissions when denying access to passwords, therefore if a password *User @ System* is stored in a folder X, and a user has access read rights to the password, but does not have access rights to the folder, the user will not be able to see the password, and any searches will not include the password. It should be noted that permissions can not be set for the top level folder because it is the starting place for all users when the log in.

Editing the password hierarchy

EPS administrators can modify the password hierarchy by clicking on the Edit Hierarchy link when viewing the password hierarchy. Clicking on this link allows administrators to edit the location of passwords and set hierarchy permissions for users and/or groups.

Whilst editing the hierarchy you can add new folders to the current level, copy, deep copy, cut, or delete sub-folders and passwords, or navigate through the hierarchy in order to make modifications elsewhere.

Copy will only create copies of things you have selected, "Deep" copy will create copies of the things you have selected as well as anything contained in the folders you have selected. For example if you have a folder called X and within it there is a password Y, if you "copy" X to another location you will get an empty copy of X. If you "deep copy" X to another location you will get a copy of X containing a copy of Y.

Administrators can also set the user and group permissions whilst editing the hierarchy. The user and group permissions are altered by clicking on the *User Permissions* tab or *Group Permissions* tab, and setting the appropriate rights for the users. Please note that user permissions will take precedence over group permissions, therefore if you deny access to a group.

Importing data from files

Users, groups, passwords, and the permissions linking them can be imported from text files using the Import options available from the menu.

The users file consists of a series of lines, each containing a user name, full name, email address, and optionally the user type and a password separated by commas. For example, importing a file containing the following three entries;

```
alice, Alice Smith, alice@secureme.info
bob, Bob Bloggs, bob@secureme.info, N, block
charlie, Charlie Jones, charlie@secureme.info, P
```

Creates a user called *alice* who is a normal user and whose password will be generated by the EPS, a user called *bob* who is also a normal user and whose password is *block*, and a user called *charlie* who is a password administrator and whose password is created by the EPS.

If an SMTP Server has been set in the configuration screen and the email address for an imported user isn't blank the user will be sent an email informing them that an account has been created for them.

Group files consist of the name of the group, a comma, and then a list of users separated by commas. For example, a file containing the following two entries;

```
group1,alice,bob
group2,alice,charlie
```

creates two groups called *group1* and *group2*, and puts *alice* in both *group1* and *group2*, puts *bob* in *group1* only, and *charlie* in *group2* only.

Passwords and permissions can be imported using the following format for each line;

```
System Name, User name, Password, Notes, Audit Policy, Record History
```

This can optionally be followed by a comma separated list of custom fields. The custom fields must be of the format `CF:name=value`.

Followed by a comma separated list of permissions. Each permission consists of a U or G to represent if the permission is for a User or Group, then a V or M to represent if that user or group should be allowed to view or modify the password, a colon, and then the name of the user or group.

The *Audit Policy* can be set to *full* for to log and send alerts for accesses, *log* to only log the access, or *none* to do nothing. If the Record History section can be either set to true to record all historical versions of the password, or false to only retain the current version.

For example a file containing the following two entries;

```
system1, username1, pwd1, some notes, full, true, UV:alice, UM:bob
system1, username2, pwd2, notes, none, false, GM:group1, UV:charlie
```

Will create two passwords both of which will be for *system1* with the following characteristics;

The first line creates an entry with the user name *username1* and the password *pwd1*, the user *alice* will be able to view the password, and the user *bob* will be able to modify the password. When users access the password the access will be fully audited (resulting in the access being logged and an alert sent), and all historical versions of the password will be recorded.

The second line will create an entry with the user name *username2*, and the password *pwd2*. The group called *group1* will be able to modify the password and the user *charlie* will be able to view the password. Accesses to this password will not cause a log message or alert to be generated, and the EPS will not store historical versions of the password.

When you import passwords they will be placed into the password hierarchy at the location you had most recently viewed.

All of the import features will display a page which allows you to select the file you wish to import, and will present you with a report once the information has been imported.

Password creation

To create passwords select the *Create* option from the *Passwords* menu. A page will be displayed which allows you to enter all of the information relevant to a password. Once you have entered all of the information requested click the *Create* button. You will then be taken to a page which will allow you to set which users and groups have access to the newly created password.

Passwords can have the *Restricted Access* feature enabled which will stop any user accessing the password without approval from one or more other users. When enabling restricted access on a password you **must** ensure that you create enough restricted access approvers. If you create a password which requires 2 RA approvers to approve access, and you only have 1 user defined as a restricted access approver, no-one will be able to access the password. Restricted Access applies to **all users**, this means that even administrators will not be able to view a password without approval if restricted access is enabled for it.

The Restricted Access also allows approvers to block a request to view a password using the *Blockers required* field. If 3 approvers have been defined, and the password has the *Blockers required* field set to 1, if any of the approvers denies the users request to view the password the users request will be denied.

It is possible to specify a set of custom fields to be included in new passwords by selecting the "Custom Fields" option under the System title from the menu on the left of the page.

Password deletion

Passwords should be deleted through the hierarchy editor. You can select the box to the left of the password or passwords you wish to delete, then choose *Delete Selected* from the *Action* drop down menu and click *Go*. Passwords are not recoverable after deletion, so do not delete passwords which you may need at a later point in time.

Password modification

You can modify a password by selecting it from either the password hierarchy, the results of a search, or any other location where you can view a password. Selecting the *Edit Details* option from the screen on which the password displayed will take you to a screen which will allow you to edit all of the details of the password.

Password restrictions

This option allows administrators to create various policies controlling the characters which must be present in passwords. An administrator can create any number of policies, and each policy can be associated with one or more passwords. The restriction policy is set by administrators when the create or edit a password.

Edit password access controls

Altering access to a password can be performed after the password has been created by selecting the *Alter Access* option when viewing a password. A page will be displayed which allows you to update the type of access that groups and users are allowed. For each user and group you wish to change you will need to select the appropriate access rights and then click the *Update group access* or *Update user access* button accordingly.

Personal Password Folder

Each user has a personal password storage area which contains password that only they can view. This area can be accessed by clicking on the "Personal" option under the Passwords title in the menu on the left of the page.

Outstanding Restricted Access Requests

The "RA Requests" option in the menu on the left shows the user any restricted access requests they have not approved or denied.

User creation

To create users manually you should select the *Create* option from the *Users* menu. You should enter the details requested in the spaces provided and click the *Create* button. Upon clicking the button you will either be shown any problems with the details supplied, or, if the creation of the user is successful, you will be taken to a screen allowing you to alter the users status, type, and group memberships.

User deletion

Users can be deleted from the system by selecting the *Delete* option under the *Users* heading. To delete a user (or group of users) you should check the box to the left of the user name and then click the “*Delete Users*” button, and then confirm the deletion.

User modification

To edit a user select the *View/Edit* option from the *Users* menu, a page will be displayed offering you a list of all the users available in your installation of the EPS. Click on the user you wish to alter and you will be taken to the user editing screen.

The user type affects how a user can interact with the EPS. An *EPS Administrator* has full access to all of the administration functions of the EPS. A *Password Administrator* only has the ability to create passwords and alter the access other users have to any passwords to which the password administrator has modification rights. A *Normal User* can only perform the actions available to them via the password access control system.

Altering the groups a user belongs to is performed by clicking on the group name. If the group is listed under the heading *Current Membership* the user is already a member of that group and clicking on the group name will remove them from the group. If a group is listed under the heading *Available Groups* then the user is not a member and clicking on the group name will make them a member of that group.

Login restrictions are based around Network Zones (which are defined by clicking on the “*Network Zones*” option in the “*System*” menu). The defined network zones are displayed and the administrator can select either “*Treat as unknown*”, “*Allow*”, or “*Deny*”. If “*Treat zone as unknown*” is selected the setting for “*Allow users to log in from unknown network zones*” in the Configuration page will determine if the user can log in from that zone or not.

User authentication

Users login passwords can be checked against external systems, but the EPS must maintain a copy of their password in order to allow the password access controls to function properly.

If you wish to use an external system to authenticate a user you should select *Authentication* from the *Users* menu, which will take you to a page showing any authentication sources which have already been defined. You may edit any of these, or you may create a new authentication source by clicking on the *Create New Source* link.

The available types of authentication source will be shown to you if you decide to create a new authentication source, you should select the most appropriate and enter the information requested. Please note that some authentication sources may require modifications to your external authentication systems, any modifications necessary will be shown on the page relating to that authentication source.

Once you have created your authentication source you can edit the user you wish to associated with the source and select the name of the source from the drop down list beside the words *Authenticated by*, you should then click on *Update Details* to store the change in authentication source.

If a user changes their password in the external authentication source and log into the EPS without changing their EPS password they will be asked to synchronize the two. Once the synchronization has taken place they will be allowed to continue as normal.

Group creation

Groups can be created manually using the *Create* option on the *Groups* menu. Once you have entered the name of the group you wish to create in the box provided you should click the *Create* button, which will take you to the screen which allows you to select which users should be part of the group.

Group deletion

Groups can be deleted using the *Delete* option under the *Groups* heading of the action menu.

Deleting a group will erase all of the access permissions any member of the group had to any of the passwords, you should therefore ensure that you are not removing a group whose access rules are relied upon for your daily operations.

Group modification

You may alter which users are part of a group after the group has been created by selecting the *View/Edit* option on the *Groups* menu.

If users are listed under the *Non-Members* heading they may be added to the group by clicking on their user name, similarly if a user needs to be removed from a group their user name will appear under the *Current Members* heading and the user name can be clicked on to remove them from the group.

Audit logs

The EPS maintains a log of accesses to passwords (where the password is set to be audited), user manipulation, and group modification. The recorded actions can be viewed using the *View* option from the *Events* menu. When you select this option a page will be displayed showing the time and date of each audit event along with the user involved, a summary of the password involved (if there was one), the action which was performed, and, if available, a tamper stamp status.

Some events can not have tamper stamps associated with them due to the action not involving a logged in user (such as failed login attempts). Where a tamper stamp is available it will show as *Untampered* if an audit log entry has been verified as not being altered outside of the EPS. If an entry appears as *Tampered* then a third party has attempted to modify the entry, and it should be treated with suspicion.

The event log can be filtered by date ranges or to a specific user. These filters are shown at the top of the log, and once changed you must click the *Update view* button to show the newly filtered entries.

The audit events can be exported by selecting *CSV File* in the drop down box beside *Output To* .:

Audit alerts

The EPS has the ability to send an Email containing details of any audited event via an SMTP Email Server. To set-up audit alerts select the *Settings* option from the *Events* menu.

There are several types of alert which can be sent via email, you should select which types of events you wish to be sent alerts about, enter the email address you wish alerts to go to, and whether or not you want to send an Email to the user involved in any actions when they are recorded in the event log.

Once you have set these options you should click "Update settings" to store these values.

If the EPS is unable to send an alert for any reason it will store the error message in the audit logs.

Configuration options

Selecting *Configuration* from the *System* menu will allow you to alter various options related to the EPS's operation. We recommend administrators visit this page in order to verify the settings comply with their existing security policies and procedures. The available settings are as follows;

Appearance

URL for your logo (optional)

This option allows you to specify the URL of an image which will be displayed in the top right hand corner of all of the EPS web pages.

Email Settings

SMTP Host

This should be set to the host name of a server through which all email notifications should be routed. This includes notifications of restricted access requests, so it is vital that you set this if you wish to use restricted access passwords effectively.

The server must be able to accept emails using the SMTP protocol, and should be able to deliver email to all of the email addresses you have associated with your users.

Emails will appear to be from

This option should be set to the address that you wish any restricted access notifications or audit alerts to come from. You should remember that users may reply to these emails and thus you may want to make this the address of a monitored list.

User Logins and Sessions

Maximum failed login attempts before an account is locked

This is the number of times a user may incorrectly enter their password before the system will deactivate their account.

Allow users to log in from unknown network zones

This can be used to stop users logging in from a network zone which not been defined using the Network Zones. Please Note; Setting this to No will stop the *admin* user from logging in. Only set this to No if you have already created another EPS administrator user.

Maximum time a user can be inactive before being automatically logged out

This sets the maximum time in minutes a user can be inactive before the system will require them to re-login.

Default Authentication Source

This sets the default authentication source for new users created either via a browser or imported.

Password Hierarchy

Hide folders containing no user accessible passwords

This setting allows you to show or hide empty folders in the password hierarchy.

Default Hierarchy Access Rule

This option allows you to allow or deny access to folders within the password hierarchy for users who do not have explicit rights to the folder.

Allow password administrators to edit the hierarchy

Setting this to Yes will allow users designated as password administrators to edit and create the folders in the password hierarchy

Password Display

Restricted access request lifetime

This specifies the maximum amount of time (in minutes) between when the user entering a reason for wishing to view a restricted access password, and when they can view it. All requests must be approved, and the user must view the password within this time. Once the access has been approved the user will have access to the password for the specified period of time.

RA approvers can vote on their own requests.

This option allows restricted access request users to vote when they try to access passwords they are restricted access request approver for.

Require a reason for a viewing password

This specifies if users viewing non-restricted access passwords should be forced to enter a reason for viewing the password.

Hide system list when editing or creating passwords

When set to Yes all users not be shown a list of already existing systems in the password creation and editing pages.

Passwords are initially

This determines if a password is initially shown or hidden when the user views the password. Showing and hiding passwords requires JavaScript to be enabled on the users browser.

Passwords shown as

This specified if passwords should be displayed as images or text.

Maximum time password is on screen

If JavaScript is enabled on the users browser this option will remove the password from the users view after the specified period of time.

Allow the use of the browser back button to review a password

This specifies if the user should be allowed to click their browsers back button to return to viewing a password after they have moved to another page.

Allow password administrators to view password audit events

If set to Yes this option allows password administrators to view a passwords event history.

Password Editing

Maximum number of days in the future an expiry date can be

This sets a hard limit for the number of days in the future an expiry date can be.

Hide password during creation and editing

If set to yes all passwords will replaced with asterisks when entering them in the password creation or editing screen, if set to no the passwords will be shown in clear text.

Reject use of historical expiry dates

If set to Yes users will not be able to enter dates in the past for the expiry date of a password.

Password Retention and Auditing

Password History Retention

This specified whether or not a user creating or editing a password is allowed to set the history retention policy for a password. If this option is set to *Choose when password is created* the user will be allowed to set the retention policy.

Password Auditing Level

This option specified if a user creating or editing a password can set the auditing policy for passwords. If set to *Configurable* the user will be allowed to set the auditing policy.

Miscellaneous Options

Separator for reports

This option sets the separator for the fields of any report generated by the EPS.

Database configuration

Selecting the *Database* option from the *System* menu will allow you to alter the access details for the database storing the passwords in the password safe. Please note that if you change the JDBC URL the information in the current database will **NOT** be transferred automatically to the new database and you will need to log in again using details valid for the new database.

Systems details

Selecting the *Details* option from the *System* menu will take you to a screen which lists several pieces of information which relate to the environment in which the EPS is running. If you wish to report a problem with your installation of the EPS you should include this information to help us reproduce the issue.

Integration modules

The *Integration* option under the *System* menu allows administrators to install integration modules and develop scripts which in turn allow the EPS to alter the passwords of remote systems. Each module may have one or many scripts associated with it which can be assigned to passwords.

For details about the scripting language used by a particular module please consult the relevant manual or information sheet for the module. For details on developing integration modules please see Appendix A.

Network zones

The *Network Zones* option under the *System* menu allows an administrator to define, edit, and delete IP address ranges which can be applied to users to control which networks a user can log in from. Network zones can be specified in IPv4 or IPv6 depending on your network infrastructure.

All passwords report

Selecting the *All Passwords* option from the *Reports* menu will allow you to download the details of all passwords stored in the system. Please note the passwords will **NOT** be encrypted and this feature should only be used when you wish to create a human readable copy of your passwords that will be stored in a safe location.

User access report

Selecting the *User Access* option from the *Reports* menu will allow you to download a comma-separated value (csv) file which contains details of the passwords users and groups have access to. The CSV file can be imported into many popular applications (such as Microsoft Excel or OpenOffice Calc).

Tips

The following are some pieces of information you may find useful whilst using the EPS

- The default inactivity before a user is automatically logged out is 30 minutes. After 25 minutes if the user has JavaScript enabled on their browser the background of the current page will change colour.
- The EPS places no special requirements on the database it uses. Any backup tool capable of correctly backing up and restoring a database from you database software can be used to backup and restore the information stored in the EPS.
- The password, group, and user data is only stored in the database, therefore moving the EPS between servers can be performed by transferring the database to an appropriate location and/or installing the EPS from scratch on the new machine.

Appendix A - Developing integration modules

It is possible to implement custom integration modules which allow the EPS to change the password on remote systems. The modules must implement the Java interface `uk.co.argosytelcrest.passwordsafe.integration.PasswordChanger`, and must be available to the EPS via the class path set by the application server.

The `PasswordChanger` interface requires the following methods to be implemented;

```
public void install(java.sql.Connection conn) throws Exception;
public void uninstall(java.sql.Connection conn) throws Exception;
public List getProperties();
public void changePassword( java.sql.Connection conn, java.util.Map pluginProperties, java.util.Map
passwordProperties, String script )throws RemoteException, IOException;
public void rollbackChange( java.sql.Connection conn, java.util.Map pluginProperties, java.util.Map
passwordProperties, String script ) throws RemoteException, IOException;
```

The `java.sql.Connection` object passed to the relevant methods provides a connection to the EPS database. We recommend that any tables you create begin with a prefix that clearly identifies them (e.g. `myldap_table`).

The `pluginProperties` Map passed to the `changePassword` and `rollbackChange` methods contains the settings the user has specified for any module specific parameters. The map key is the internal name for your module property, and the value is a String containing the value the user has set for this password.

The `passwordProperties` Map passed to the `changePassword` and `rollbackChange` methods contains values specific to the password being changed. These are;

Key	Value
username	The user name associated with this password.
old_password	The original value for the password.
new_password	The value the password should be changed to.
system	The system on which the change should take place.

The `script` String passed to the `changePassword` and `rollbackChange` methods contains the script to be executed for this password.

The `getProperties` method returns a List of `uk.co.argosytelcrest.passwordsafe.integration.PasswordChangerProperty` objects which contain the details of the properties specific to the integration module. `PasswordChangerProperty` object should be constructed using the following constructor;

```
public PasswordChangerProperty( String internalName, String displayName, String description, String
defaultValue )
```

Where `internalName` is the name that will be used for the parameter when the `pluginProperties` Map is constructed, `displayName` is the name shown to the user when they are asked to set the values which will be held in the `pluginProperties` Map, `description` is an optional description which is currently not used, and `defaultValue` should contain a sensible default for the property

Appendix B – External API

The EPS allows users to search for, fetch, and update passwords within the database using HTTP. All parameters must be passed using HTTP POST, and all results will be returned in the body of the response.

Common Parameters

The parameters used by all of the calls are as follows;

Name	Contents
username	The name of the user the request should be audited under.
password	The users password.

Searching

URL : [http://\[servername\]/passwordsafe/api/FindIds](http://[servername]/passwordsafe/api/FindIds)

Additional Parameters

Name	Contents
searchUsername	The username of the password required.
searchSystem	The system the password is on.

Response

The response will contain the id or ids of the passwords with the given username in the given system.

Fetching the password

URL : [http://\[servername\]/passwordsafe/api/GetPassword](http://[servername]/passwordsafe/api/GetPassword)

Additional Parameters

Name	Contents
id	The id of the password to fetch.

Response

The password. The response will **only** contain the text from the password field.

Updating

URL : [http://\[servername\]/passwordsafe/api/UpdatePassword](http://[servername]/passwordsafe/api/UpdatePassword)

Additional Parameters

Name	Contents
id	The ID of the password to update.
newPassword	The value to set the password field to.

Response

The password. This response should always match the value set in newPassword.