FUSION SECURITY

User Guide

FUSION SECURITY
User Guide

This guide provides information on how to create, maintain, and delete user accounts from Fusion Security.

Fusion Security Version: 2.X
Document Last Updated: May 14th 2018

Version: 20180514

Contents

1 User Accounts

Fusion Security can be used to manage user accounts across the Fusion product range. Changes to user accounts in Fusion Security will become effective immediately in any of the Fusion Products that are secured with Fusion Security.

Fusion Security must be configured to communicate to an SDMX Structure source (this may be a Fusion Registry) in order to obtain a list of Data Providers, Data Consumers, and Agencies. Connecting to a structure source is covered in the installation guide. When creating a user account, it is possible to assign the user to zero or more SDMX organisations (Data Provider, Data Consumer, Agency).

Any user may also be assigned the role of Admin. Admin access gives higher privileges to other Fusion tools such as Fusion Audit and Fusion Registry.

Fusion Security also provides an additional privileged user account, called the “root user” (userid ‘root’) who is an administrator with all of the privileges that go along with it. The root user may not be deleted, but he can be locked. The root user also has the ability to import or export user information from Fusion Security (see section 3) and has the ability to modify any other user account. The root user is not visible to administrator users, so if logging into Fusion Security as an administrator user, the root user will not be displayed. It is recommended to use administrator accounts for user administration, and only use the root user if absolutely required, for example if the administrator password(s) are forgotten. It is highly recommended to change the root user password or lock the root account as soon as possible.

User accounts may be enabled or disabled by an administrator though the UI. User accounts may additionally be locked or unlocked. An account will be locked automatically by the system if a user tries to log into their account with the incorrect password an excessive number of times. By default there is no maximum limit set, this can be configured as required. An account can only be enabled/disabled or unlocked using the UI.

It is possible to restrict accounts to only authenticate if the login is from certain IP addresses. A failed login due to IP restriction will be counted as a failed login attempt, and an excessive number of consecutive login failures may cause the user’s account to be locked.

2 User Administration

2.1 Overview

Only users with root or admin permission can login to the Fusion Security user interface. Access from any other user account is prohibited.

To administer accounts first log in to Fusion Security via the web interface.

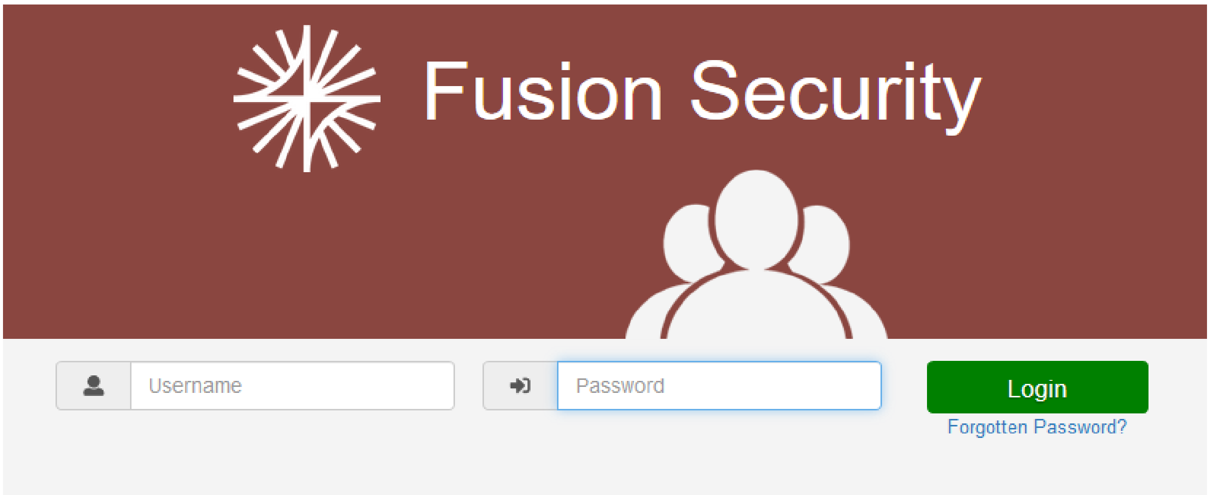
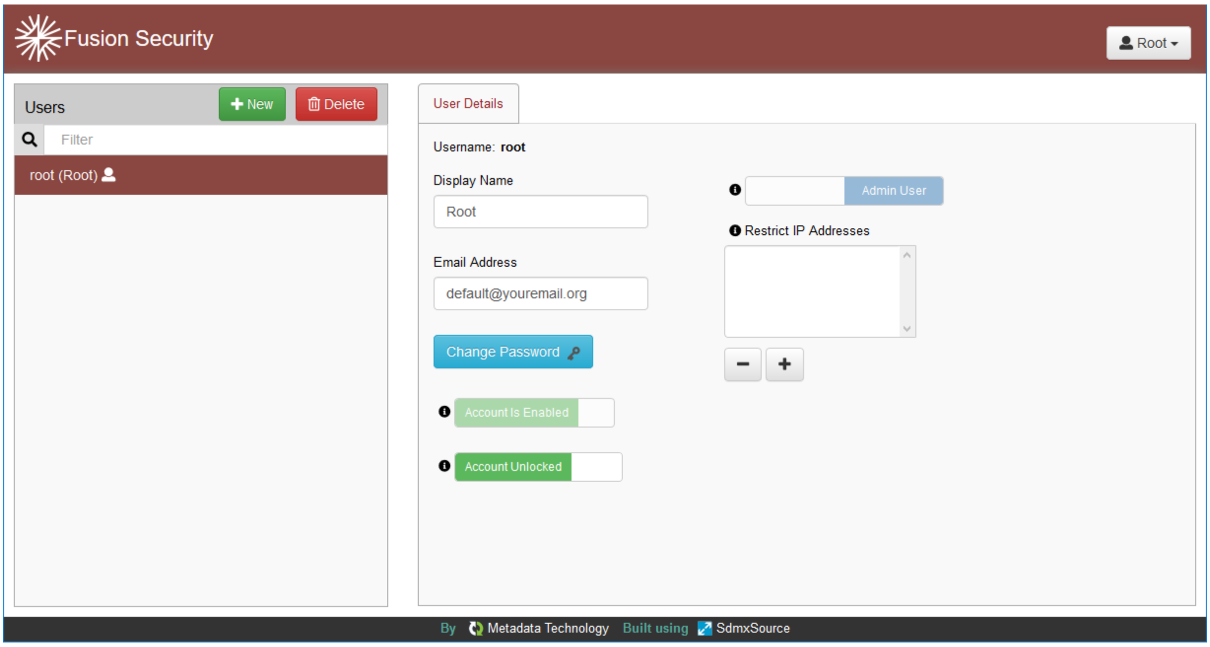


Figure 1: Showing the Fusion Security login page

The home page will show a list of all the users in the system. Users are listed by username and the display name is shown in brackets (unless username and display name are the same).



Username: **root**

Display Name: Root

Email Address: default@youremail.org

Figure 2: Showing the Fusion Security home page

Modifying a user's details is simply a case of clicking on the appropriate control (e.g. the *Enable Account* control) and the change is made to that user. The only exceptions to this are 'Display Name' and 'Email Address'. These controls have their own "Save" button which is displayed when a change is made to the value.

2.2 Creating a New User

Click on New User, a popup dialogue will appear. Ensure all fields in this dialogue are filled in before clicking 'Add User'. The characters allowed in the username include all alphabetic, all numeric and the characters: underscore (_), dollar ($) and hyphen (-).

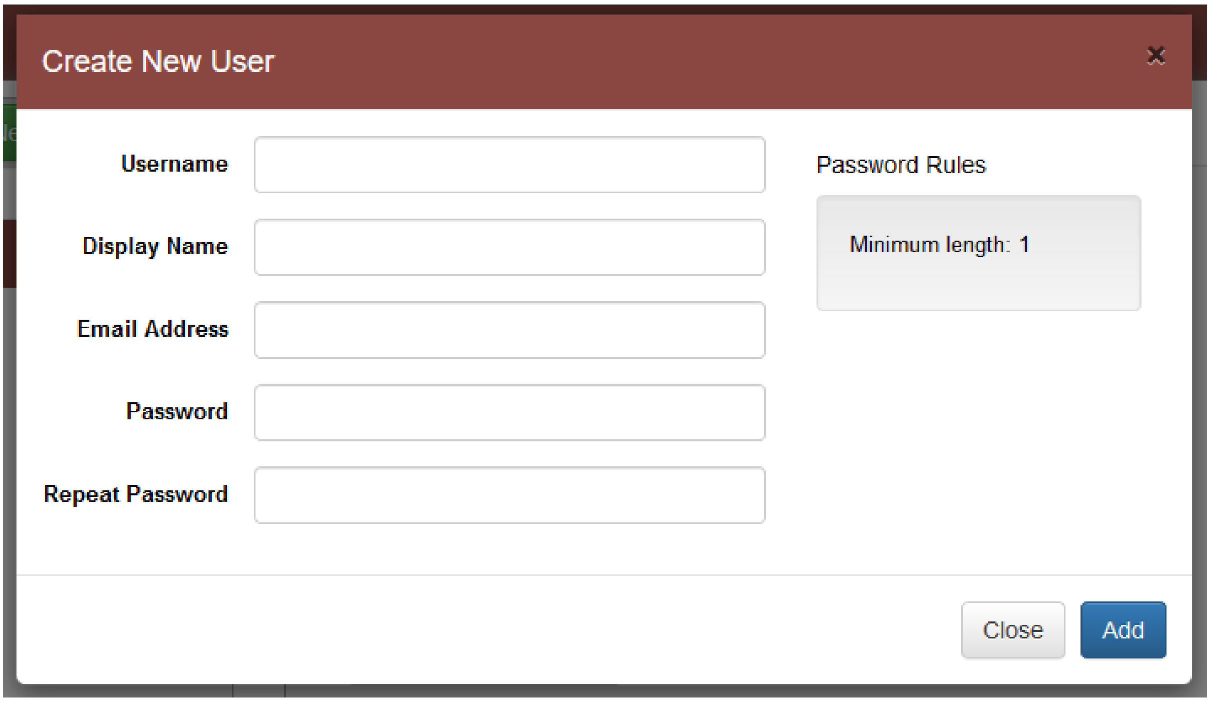


Figure 3: Showing the New User dialogue

The username for each user must be unique and cannot be changed once set. The display name for each user does not have to be unique and can be modified at a later date from the "User Details" screen.

The password rules are displayed on the right-hand side of the dialog. These rules are configurable, as discussed in the installation guide. On form submission Fusion Security will additionally verify that the password supplied is not contained in the list of illegal passwords: these are passwords which are deemed unsafe due to their simplicity or commonality

On successful creation of a new user account, the pop up dialogue will close, and the user will be added to the list of users displayed in the area in the left-hand side of the screen.

The user's account will be enabled, but at this stage of user account setup the user will not be assigned to any organisations. Organisation assignment will provide the user with specific roles. The Fusion products may require that certain actions have a specific role, e.g. only a Data Provider can register data. It is not mandatory to assign a user to an organisation, however this may restrict what access rights the user has in secured systems.

2.3 Assigning a User to Organisations

A user's account can be assigned to zero or more organisations, allowing the user to assume the role of an organisation type (e.g. Data Provider) when using a Fusion application. To assign a user to an organisation first select the user, then click the 'Organisations' tab. Note that the root user is the only user that cannot be assigned to an organisation, as the root user has full access privileges. The Organisations view will show a hierarchical tree of all the organisations known to the Fusion Security application. These organisations are obtained from the Structure repository. The changes will be immediate in any Fusion application that has been configured to use Fusion Security.

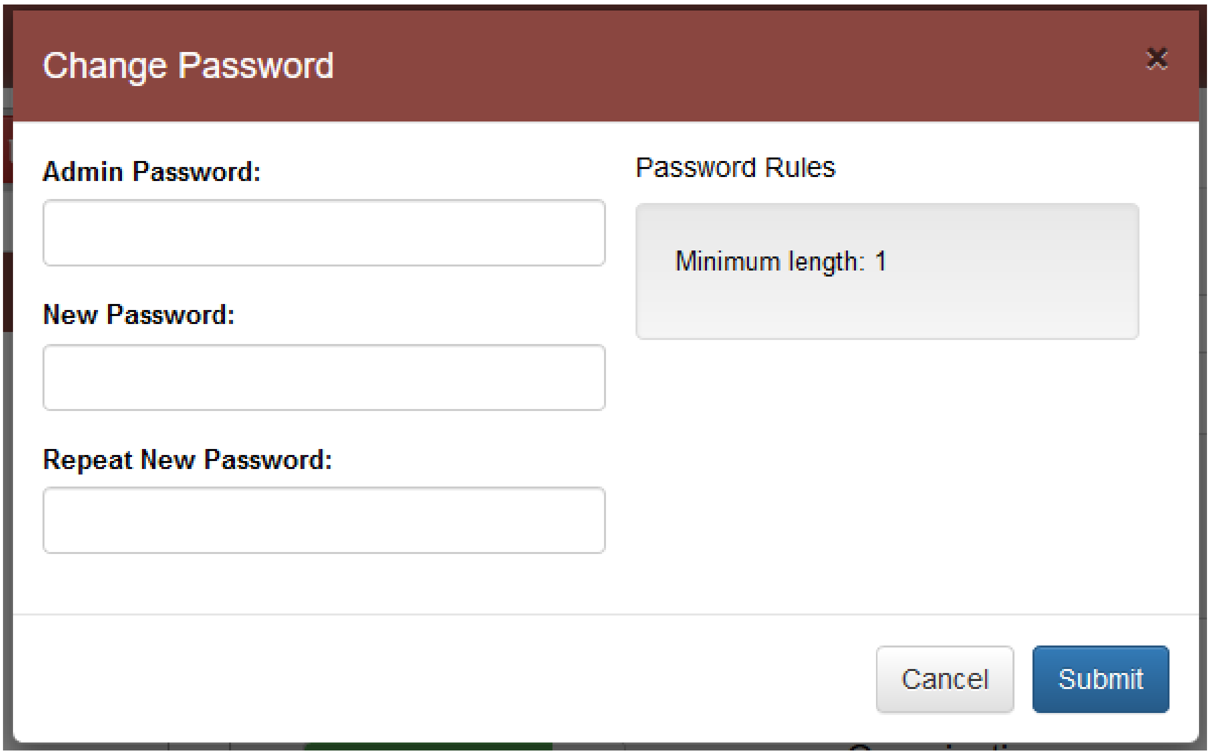
2.4 Enabling Admin Privileges

It is possible to promote a user to 'admin' status by clicking the 'Admin enabled' checkbox under the 'User Details' tab. Admin users have the privilege of being able to log into Fusion Security and are able to maintain any user account, including other admin users. The root user is not visible in the UI to any other users and so cannot be modified by any other user.

2.5 Changing a Password

As part of the administration function admin users can change the password of any user in the system, except for the root user. Root users are allowed to change any user password. It is not possible to discover what a user's password is as it is encrypted on the server using a strong one way hashing algorithm.

To change a password, first select the user and then click on the 'Change Password' icon under the 'User Details' tab. A pop up dialogue will be displayed, allowing the user's password to be changed. The admin user must re-enter his own password before this operation will be allowed to succeed. The password verification rules are the same as the rules enforced on account creation.



Change Password

Admin Password:

New Password:

Repeat New Password:

Password Rules

Minimum length: 1

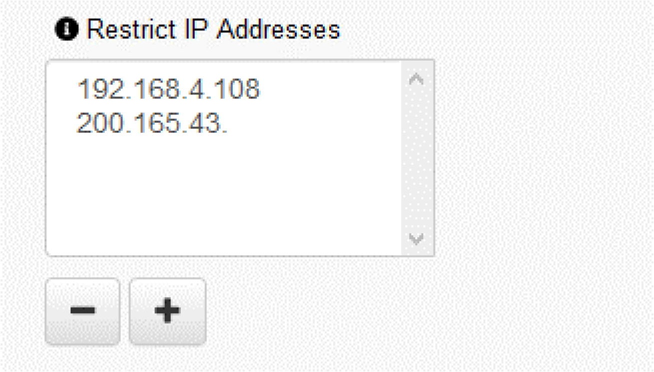
Figure 4: Showing the change password dialogue

2.6 Changing display name, and email

It is possible to change the display name, and email address for a user. It is not possible to change a user's username. To change either the display name or email address select the user's account, and modify these entries in the ‘User Details’ tab. Click the ‘Save’ button to action these changes. If an invalid display name (such as an empty display name) or email is entered, then an appropriate error message will be displayed.

2.7 Restricting IP addresses

It is possible to restrict a user’s account so that the user can only log in from computers which match the restricted IP address. The IP address specified may contain wild-carded fields. To restrict a user’s account in this way, select the user, and click the add icon under ‘Restrict IP Addresses’.

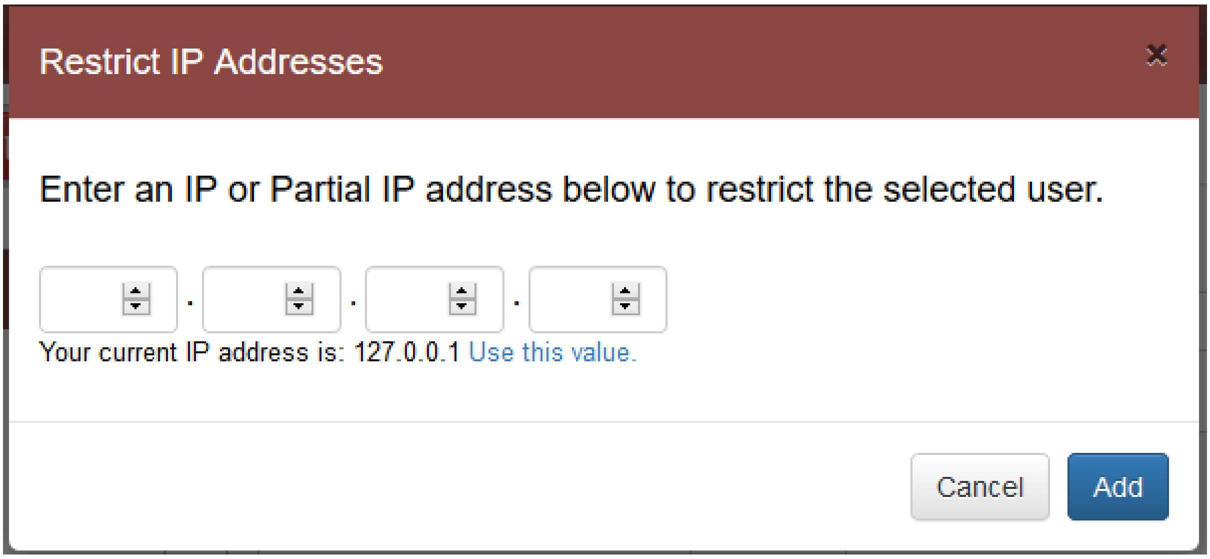


Restrict IP Addresses

192.168.4.108
200.165.43.

Figure 5: Showing a list of restricted IP addresses, one is wildcarded

A pop up dialogue will appear prompting for a full or partial IP. To wildcard part of the IP Address, simply leave it blank, as shown in *Figure **6*** below. On completion, click ‘Add IP’ which will have the effect of closing the dialogue, and adding the IP to the list. The change will become effective immediately. You may repeat this process to add as many IP addresses as you like against a particular user.



Restrict IP Addresses

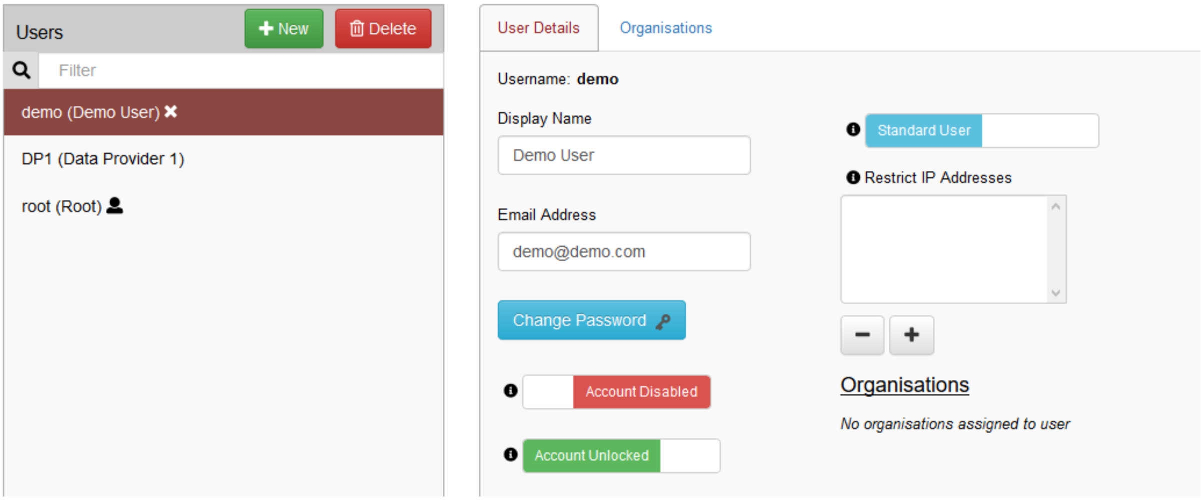
Enter an IP or Partial IP address below to restrict the selected user.

Your current IP address is: 127.0.0.1 Use this value.

Figure 6: Showing a partial IP address with a wildcarded last field

2.8 Disabling/Enabling an Account

A user’s account may be disabled. A disabled account will prevent the user from logging into any Fusion application with their login credentials. To disable or enable an account, select the user and check/uncheck the ‘Account Enabled’ checkbox. The user’s name in the list or users will have an ✖ icon next to it if the account is disabled.



demo (Demo User) ✖

DP1 (Data Provider 1)

root (Root)

Username: **demo**

Display Name: Demo User

Email Address: demo@demo.com

Account Disabled

Account Unlocked

Standard User

Restrict IP Addresses

Organisations

No organisations assigned to user

Figure 7: Demo User's account is shown as disabled

2.9 Locking/Unlocking an Account

A user's account may be locked and unlocked. A locked account will prevent the user from logging into any Fusion application with their credentials. An account is locked automatically after an excessive number of failed login attempts to any Fusion application. To lock or unlock an account, select the user and click the 'Lock/Unlock' button at the top of the page. The account will be locked/unlocked with immediate effect. The user's name in the list of users will have an 🔒 icon next to it if the account is locked. **Note:** If the ROOT Account is locked, then this can only be unlocked by using the command line application "FusionSecurityCL" which is discussed in the Set-Up Guide.

2.10 Deleting an Account

To delete an account, select the user to delete, and click the 'Delete' button at the top of the page. A confirmation dialogue will appear. It is important to note that once confirmed a delete operation cannot be undone. It is important to note that the delete operation does not delete any SDMX Organisations from the structure source: it deletes only the user account that may have been linked to an Organisation(s).

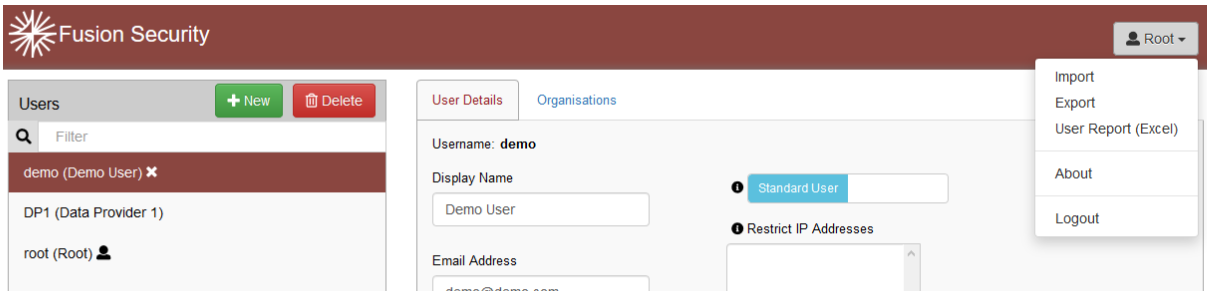
3 Importing and Exporting User Information

3.1 Introduction

There are 3 ways to make a copy of the information persisted by Fusion Security:

1. The database that Fusion Security is communicating with can simply be backed-up in the usual manner.
2. Fusion Security provides the ability to import and export user information with the aim of allowing information from one Fusion Security instance to be easily applied to another instance without the necessity for performing database requests and uploads.
3. A dump of all users can be performed in Excel format. Note that this cannot be used for import purposes by can be used as a record of the state of Fusion Security at a particular time.

3.2 Import and Export (SDMX Format)



Username: demo

Display Name: Demo User

Email Address

Figure 8: Showing the Import and Export functions

Clicking Export will attempt to download all of the user information from Fusion Security. The actual behaviour of what happens is dependent on the behaviour of your browser: your browser may automatically download the file to a particular directory or it may prompt you for the name and location of the file to save the information to.

Once saved to hard-disk the file can then be backed-up as you require.

To import a saved file, use the Import function. A dialog will be displayed requesting a file to be loaded. This should be a file previously exported from Fusion Security. Once loaded in, the new users will be in your Fusion Security system.

There is an important point to note when importing user information. When the import occurs, only users which do not already exist in Fusion Security will be imported from the file. This prevents the root account from being updated with information from the old system. If you wish to overwrite existing users, please delete them from the Fusion Security system before performing the update.

Please note that passwords are encrypted in the exported file. When the user information is applied to a new instance of Fusion Security the passwords will work as they did previously.

3.3 User Report (Export in Excel Format)

Clicking the *User Report (Excel)* control will attempt to download the user information from Fusion Security. The actual behaviour of what happens is dependent on the behaviour of your browser: your browser may automatically download the file to a particular directory; it may prompt you for the name and location of the file to save the information to; it may automatically open Microsoft Excel and show the contents of the file.

Once activated an Excel spreadsheet is generated with columns for the following:

- Username – the username of the user, which the user would use to log in to a Fusion Product.
- DisplayName –used for presentation purposes only and is not used for login purposes.
- Email address – used to contact the user for forgotten passwords, etc.
- Role – either states ADMIN (showing that the user is an Admin), ROOT USER (states that the user is the Root user) or this cell is blank showing that this user is neither an Admin or the Root user.
- The Organisation Location (Domain) – the domain that the user has got organisations for
- The Organisations assigned to the user – the individual organisation type (Data Providers, Agencies, Data Consumers) and the id of the organisations are listed here

Note that the passwords for each user are not exported in the report. This Excel file cannot be used to load information back into Fusion Security.