✳ virus exchange

Virex Sharing Application

Installation and Usage Guide

☂AVIRA

Trademarks

Windows is a registered trademark of the Microsoft Corporation in the United States and other countries. All other brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. This does not mean, however, that they may be used freely.

✱ virus exchange

Table of Contents

1. Introduction

Virex is a web-based application based on the Norman Sample Sharing framework to organize the exchange of malicious samples, clean samples and URLs. Virex offers various statistics, such as the amount of downloaded samples by a sharing partner, the number of newly added samples by the owner of the system as well as file size and traffic metrics.

The application contains a complex user management for internal as well as for external users. It supports enabling and disabling user accounts, changing PGP keys, limiting the rights of the sample sharing to different collections types as (e.g., malware, clean and URLs). Additionally, there is a user account history, which shows the last requested samples and the last requested list of MD5 hashes. The downloaded samples for each user can be limited by date. This means that starting an exchange with a new sharing partner can start at a predefined date.

The source code is published under the New BSD License (Reference: http://www.opensource.org/licenses/bsd-license.php) and is hosted on Google Code http://code.google.com/p/virex/.

On the Google Code project you can create new issues if you find a bug or encounter other issues in the application. You can check out the code from the GIT repository and feel free to commit code changes. We will publish updates, if necessary, on the Google Code project page.

This installation and usage guide will help you install and use the application on your own server as well as provide some information about the application.

2. System Requirements

The Virex application was designed to run on UNIX and Microsoft Windows operating systems. In either case, you need the following additional software:

- Apache (http://apache.org/)
- PHP5, including the following extensions (http://www.php.net/)
    o Reflection
    o PCRE
    o SPL
    o PDO
    o PDO MySQL
    o GD
    o Fileinfo
- MySQL (http://www.mysql.com/)
- Yii PHP framework (http://www.yiiframework.com/)
- Fusion charts (http://www.fusioncharts.com/)
- SMTP server
- GPG (http://www.gnupg.org/)
- 7zip (http://7-zip.org/)

The location of 7zip and GPG must be inserted in the PATH environment variables to work properly.

3. Configuration

This section describes the required configuration for the different modules to install the application on your web server.
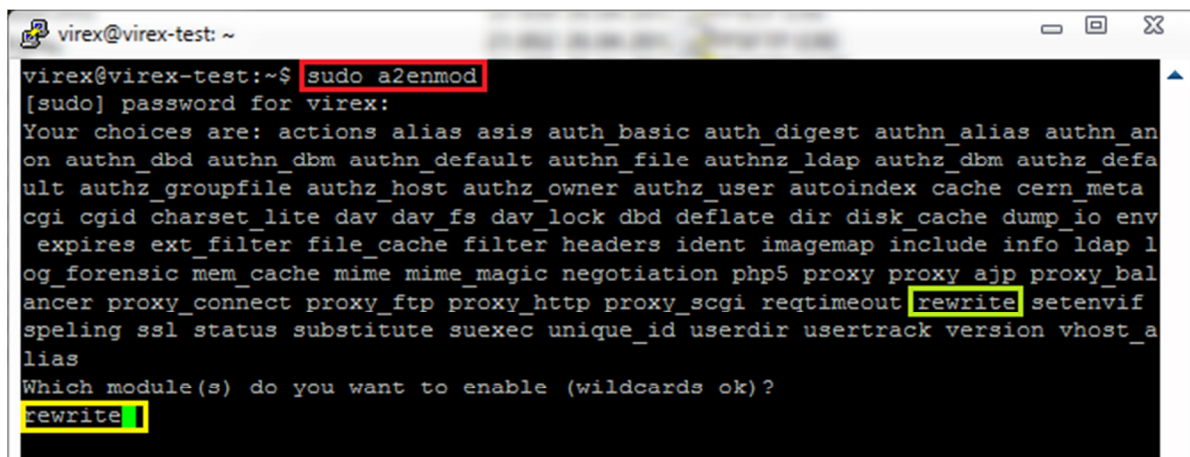
3.1 Apache

For the Virex application to work properly, you must be running Apache. In addition, the following options need to be adjusted:

3.1.1 Rewrite Module

The rewrite module (Reference: http://httpd.apache.org/docs/current/mod/mod_rewrite.html) must be enabled for the Virex application. Please open the **httpd.conf** file in a text editor, search for the line **LoadModule rewrite_module** and uncomment the entry.

> If the configuration file is empty on your server, please use **sudo a2enmod** to start the Apache configuration wizard in the terminal. Type the name of the module(s) you want to enable, then confirm your changes by pressing return (as shown):
>
>

3.1.2 AllowOverride Directive

The **AllowOverride** directive (Reference: http://httpd.apache.org/docs/2.0/mod/core.html#allowoverride) must be changed to **AllowOverride ALL** for the directory where the Virex application is located. Please open **/etc/apache2/sites-available/default** in a text editor and add the directive. This is how it should look:

```
<Directory %path_to_Virex%>
     Options Indexes FollowSymLinks MultiViews
     AllowOverride All
     Order allow,deny
     allow from all
</Directory>
```

Note: Apache must be restarted for the changes to take effect.

3.2 MySQL Database

The Virex application requires a MySQL database to store information related to all samples, users and statistics. The database can be created using the command line interface of your operating system and the MySQL software.

First start the MySQL prompt and authenticate yourself:

```
mysql –h hostname –u root -p
```

The second step is to create a new database. The name can be chosen freely. We are using **db_name** as a placeholder in this guide.

```
CREATE DATABASE IF NOT EXISTS db_name;
```

To enable communication between application and database, a new user should be created. You can use the following command (username and password are placeholders):

```
GRANT ALL PRIVILEGES ON db_name.* TO 'username'@'localhost' IDENTIFIED BY 'password';
```

3.3 PHP

The application is using different PHP modules, they either need to be enabled in the configuration or installed on the server. If you are using PHP 5.3 or above, the following modules are already part of the PHP core and are enabled by default.

- Reflection (http://www.php.net/manual/en/reflection.installation.php)
- SPL (http://www.php.net/manual/en/spl.installation.php)
- FileInfo (http://www.php.net/manual/de/fileinfo.installation.php)
- PCRE (http://www.php.net/manual/en/pcre.installation.php)

The following extensions are not part of the PHP core and must be added manually:

- PDO (http://www.php.net/manual/en/pdo.installation.php)
- PDO MySQL (http://www.php.net/manual/en/ref.pdo-mysql.php)
- GD (http://www.php.net/manual/en/image.installation.php)

Please search for the PHP configuration file **php.ini** and open the file in a text editor. Enabling and disabling an extension can be easily done within this configuration file:

```
#extension=%extension_name%.so (UNIX)
#or
#extension=%extension_name%.dll (Microsoft Windows)
```

To enable the extension, just remove the **#** which is the comment in the PHP configuration file. If one of the required extensions is not yet installed, please refer to the installation extractions above.

Note: Changes in the **php.ini** file require a web server restart to take effect.

3.4 Yii Framework

The Yii framework is a high-performance PHP framework and is used by the Virex application. It's required that you install the Yii framework to use the Virex application. Please download the latest release from the Yii project page:

http://code.google.com/p/yii/downloads/list

Unpack the archive and upload the unpacked content from the archive to the Virex **htdocs** directory. There is no additional configuration necessary.

3.5 FusionCharts

FusionCharts is a framework for creating charts using JavaScript and Flash. It is available as a free or paid version. The free version provides basic charts (i.e., 3D charts are not available), but it is enough for visualizing ideas.

The free version can be downloaded from:

http://www.fusioncharts.com/goodies/fusioncharts-free/download/

The extended version can be downloaded as a trial version here:

http://www.fusioncharts.com/download/trials/
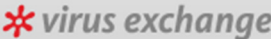
Similar to the installation of the Yii framework, the archive needs to be unpacked and the unpacked content from the archive needs to be uploaded to the Virex **htdocs** directory. There is no additional configuration necessary.

4. Installation

After configuring the required software, you can upload the Virex sources to your htdocs directory and continue with the installation.

Please access your web server using the IP or the URL. You will be automatically redirected to the installation script.

The installation page looks like this:

The installation script will verify that all requirements are fulfilled and guide you through the installation process. All satisfied requirements are indicated by a green check mark.

To finish the requirements check successfully, please create the following directories:

- htdocs/assets
- protected/runtime
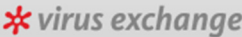
and grant write access where your web server is running for those directories. Under Unix it can be done this way:

```
sudo mkdir htdocs/assets protected/runtime log
sudo chown root:apache htdocs/assets protected/runtime log
sudo chmod 775 htdocs/assets protected/runtime log
```

![virus exchange logo]

After reloading the page the installation script will check again if the requirements are fulfilled and you can continue the installation.

In the next steps, you will enter some basic information, including the database. The page looks like this:

The **Database** section contains all the information about your MySQL database, which was created earlier in this document. If you forget the details, please check your history or server.

The **Paths** section contains the paths to the Yii framework, the path where you like to store your samples, the path where you will upload new archives to the database and a temporary path for some required operations (e.g., unpacking).

The administrator account will be automatically created after the installation and is required to login to the system. Please enter a valid email address and password.

After finishing the configuration wizard, please click the **Install** button to create the configuration file. If a directory doesn't exist, you will receive an error message which could look like this:

Configuration

Errors:
- The storage path does not exist and could not be created: /local/web/virextest.avira.com /storage

Please resolve any problems and try the installation again.

If the check of the given configuration was successful, a new page will open with the PHP code for the configuration file. It will look like this:

virus exchange
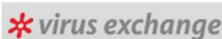
Installation

Configuration

Please write the following lines in: **/local/web/virextest.avira.com/protected/config/config.inc.php** and click **Done**

```php
<?php
// Paths
define('VIREX_YII_PATH', '/local/web/virextest.avira.com/yii/framework/yii.php');

define('VIREX_STORAGE_PATH', '/local/web/virextest.avira.com/storage');

define('VIREX_INCOMING_PATH', '/local/web/virextest.avira.com/incoming');

define('VIREX_TEMP_PATH', '/tmp');

// DB config
define('VIREX_DB_HOST', 'localhost');

define('VIREX_DB_NAME', '    ');

define('VIREX_DB_USER', '    ');

define('VIREX_DB_PASS', '    ');

// Other
define('VIREX_URL', 'http://virex.apl.com');

define('VIREX_PASSWORD_SALT', 'dh8ivpicmu5sosowrew4terekam9apefe');
```

Done

UNIX systems: You have to copy the PHP code and paste the code to the configuration file, which has to be created. Save it to **protected/config/config.inc.php** and press the **Done** button.

Windows systems: The configuration file will be created automatically. You can continue by pressing the **Done** button.
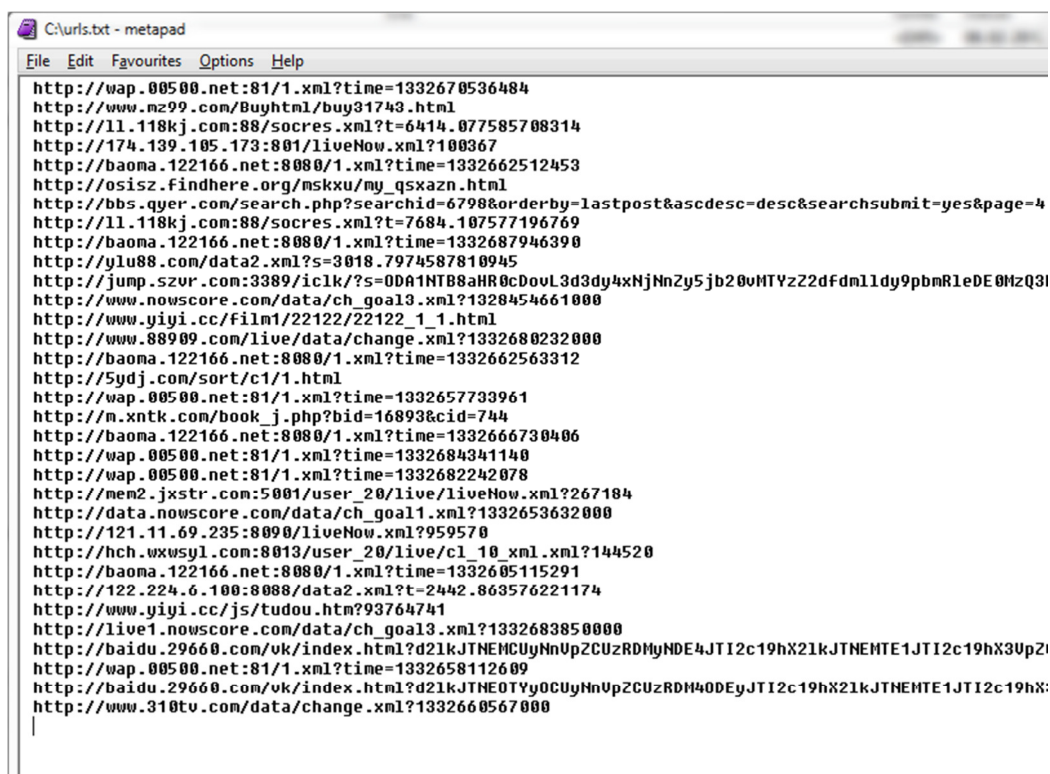
To create the initial folder structure for the incoming directory, run the following command on the command line:

```
/usr/bin/php %path_to_virex%/protected/commands/console.php archives show
```

The following directories will be created (including subdirectories):

+ clean	+ detected

- bogus
    - daily
    - monthly
	- bogus
	    - daily
	    - monthly
	    - urls

- **bogus**
  The bogus directory contains archives/files which couldn't be processed.

- **daily**
  All samples uploaded to the daily directory will be shared with users, which have the right to download daily collections.

- **monthly**
  All samples uploaded to the monthly directory will be shared with users, which have the right to download monthly collections.

- **urls**
  To share URLs via Virex, you have to upload a text file (containing the URLs in plain text) to this folder. The URLs will be shared with each user who has the right to download URLs.

If you also want to share clean samples using the Virex framework, you have to grant users the right to download clean samples.

5. Cronjobs

The cronjobs will automatically process new archives with malicious or clean files and automatically process URLs. All cronjobs use the PHP script **console.php**, which is located under **protected/commands/**.

If you are running the Virex application on a Ubuntu server, you can use **sudo –crontab –e** to start the cron table. It's also possible to edit the file **/etc/crontab** directly using a text editor.

5.1 Process Archives

We recommend setting up a job to check every 10 minutes for a new archive in the incoming directory with:

```
*/10 * * * *        /usr/bin/php %virex_dir%/protected/commands/console.php archives process &>>
%virex_dir%/log/archives_process.log
```

5.2 Pending Samples

This job is needed to check if pending actions are set in the database (delete file from database, etc.)

```
*/10 * * * *       /usr/bin/php %virex_dir%/protected/commands/console.php php samples pending &>>
%virex_dir%/log/samples_pending.log
```

5.3 Weekly Statistics

If you want to receive a weekly statistics email, you can set up the new job this way:

```
0 23 * * 0        /usr/bin/php %virex_dir%/protected/commands/console.php samples weeklystats &>>
%virex_dir%/log/samples_weeklystats.log
```

Weekly statistics are generated every Sunday at 23:00.

5.4 Update Statistics in Database

This job updates the traffic/download statistics in the database.

```
0 */3 * * *              /usr/bin/php %virex_dir%/protected/commands/console.php dbmaintenance
update_stats &>> %virex_dir%/log/dbm_update_stats.log
```

This job runs every 3 hours.

In these examples **%virex_dir%** is used as a placeholder. Please replace it with the corresponding path on your server.

6. Upload Samples

To upload samples to your Virex system you can either use the FTP/SFTP protocol or use the incoming folder as a network share.

The uploaded archive should be a ZIP archive. The Virex internal unpacker checks the uploaded archive with 200 levels of recursion.

If you want to upload new URLs to the system, you have to upload a text file to the **urls** folder in the **incoming/detected** directory. The URLs have to be inserted in plain text.

The uploaded files will be shared depending on the folder they were uploaded to.

- **incoming/detected/daily** will be shared with all users with "Rights Daily"
- **incoming/detected/monthly** will be shared with all users with "Rights Monthly"
- **incoming/detected/urls** will be shared with all users with "Rights URLs"
- **incoming/clean/daily** will be shared with all users with "Rights Daily && Rights Clean"
- **incoming/clean/monthly** will be shared with all users with "Rights Monthly && Rights Clean"
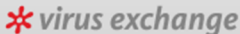
The fastest method to process the archive is to upload an archive where all files are in the archive's root.

7. Registration process for external users

On the Virex login page you can find a link **Create new account!** This link allows external users to register an account on your system.

The user has to enter the following information in the formula field:

- Username (used for downloading samples via the Sample Sharing client)
- Company
- Email address
- Password
- Public PGP key
- Verification code

Register

Username *

Company *

Email *

Password *

Confirm password *

Public PGP Key *

Verification Code *

sdacuh

Get a new code

Please enter the letters as they are shown in the image above.
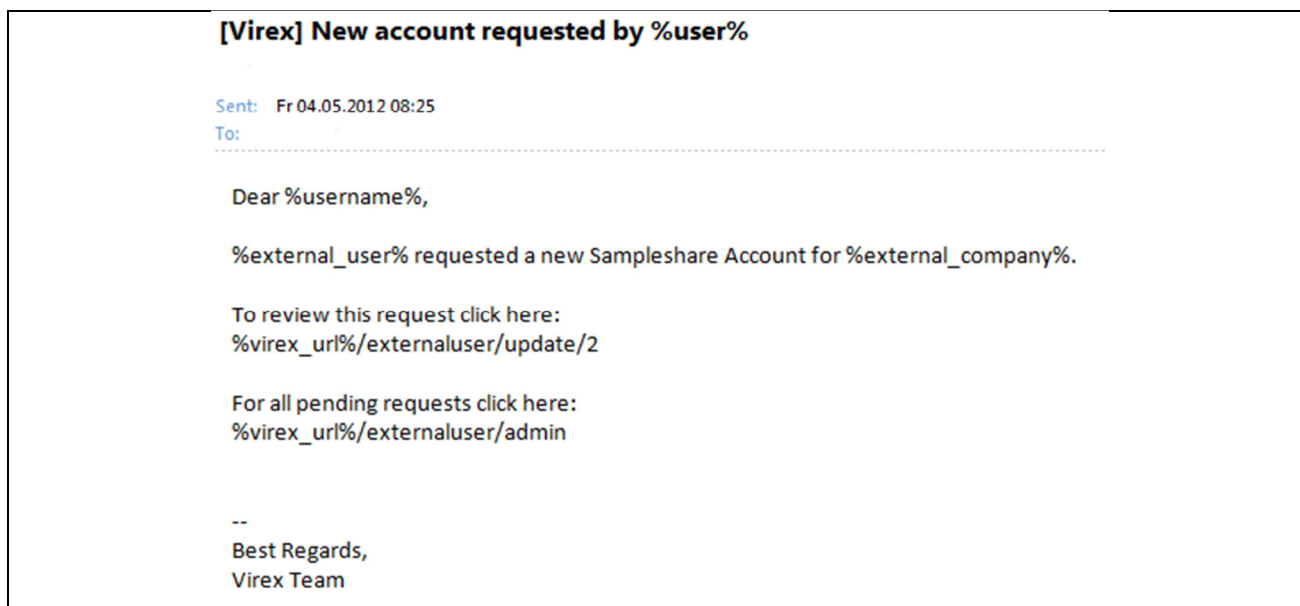Letters are not case-sensitive.

Submit

Already have an account?
Reset password!

After pressing the **Submit** button, the system sends a registration link via email to the user's email address. Once the email address is verified, the account will get the status "Pending" in the external users overview site. A notification email will also be sent to all internal users who have the **New account notification** option enabled in their profiles.

If an external user has registered a new account and verified his email address by clicking a link in an initial sent email, the internal users will get a notification email from the Virex system. This email looks like this:

[Virex] New account requested by %user%

Sent: Fr 04.05.2012 08:25
To:

Dear %username%,

%external_user% requested a new Sampleshare Account for %external_company%.

To review this request click here:
%virex_url%/externaluser/update/2

For all pending requests click here:
%virex_url%/externaluser/admin

--
Best Regards,
Virex Team

The words in "%" are placeholders, which will be replaced by the Virex system automatically.

8. External User interface

After a successful login on your system, the external user has access to a basic web interface. It offers the possibility to search for MD5 hashes, as well as download the Sample Sharing client.

This looks like:
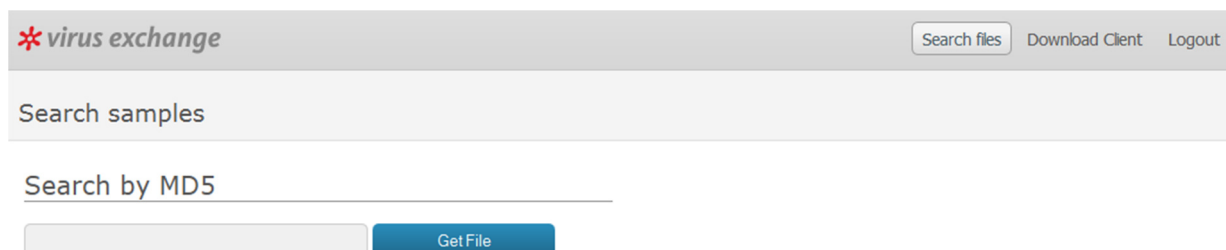
If the searched MD5 is known in your system, the encrypted file will be offered for downloading.

8.1 Download Client

The user is able to download a prototype of the Norman Sample Sharing Client Framework.
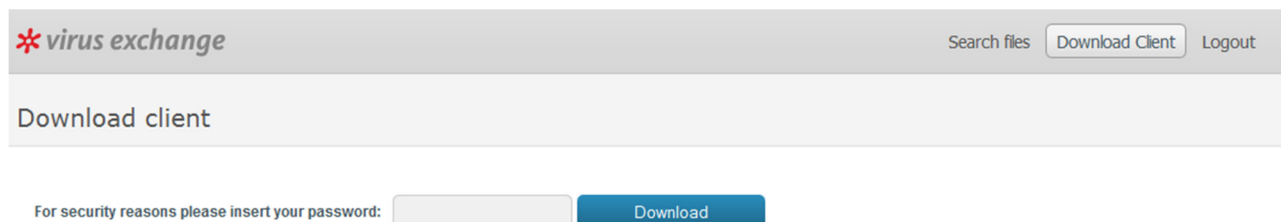
After authenticating with the correct password, the site offers the Client Framework scripts for downloading.

The downloaded scripts contain the following information:

- Username for downloading from your system
- Password for this user
- URL to which the client script should point

The external user has to insert the password for his uploaded PGP key in the **sampleshare.php** script.
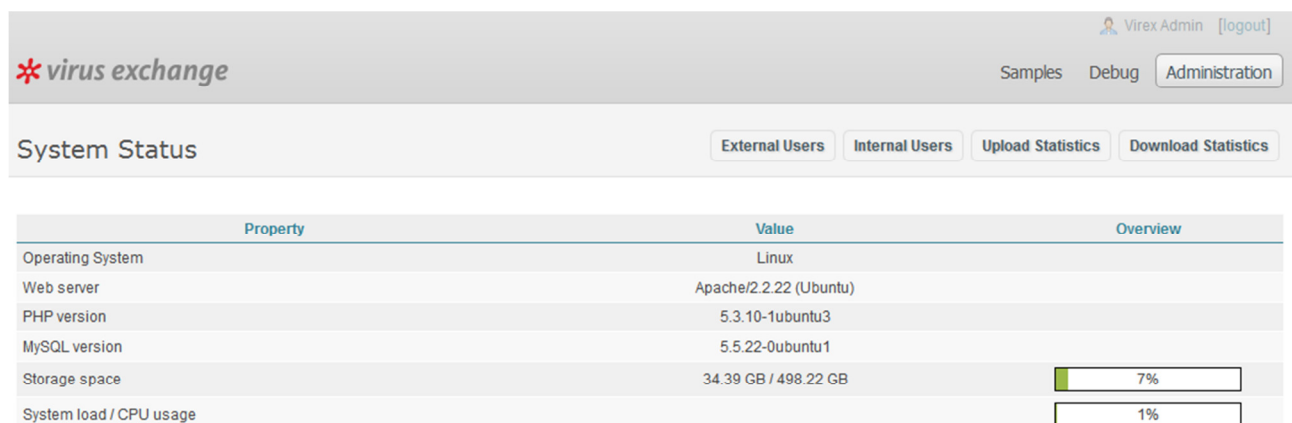
This looks like:

"define('GPG_PASSPHRASE', 'your_passphrase'); // change this to your gpg passphrase"

9. Usage

The Virex web interface offers you the function to view the samples, manage the debug samples and to manage the internal as well as the external users and view statistics.

The start page of the web interface looks like this:

9.1 Samples

The **Samples** view provides information about all uploaded samples and URLs. You can switch the view by clicking the **Detected**, **Clean** or **URLs** button. The displayed tables look similar in each view.

It is possible to perform different actions on a sample.

 Clicking this icon disables a single file for sharing. The file is still present on the system, but an external user cannot download it.
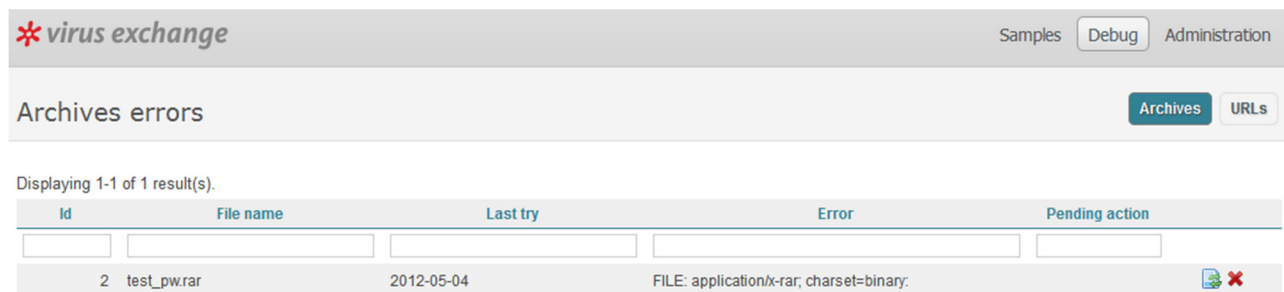
 Clicking this icon removes a file from the database as well as the file storage.

The functionality is similar in the **Clean** and **URLs** table.

Clicking on **Click here to restrict results to a specific time frame** opens a menu where you can select a time frame. Afterwards only files uploaded in this time frame will be displayed.

9.2 Debug

The **Debug** view provides information on broken archives or URL text files. You can switch the view by clicking the **Archives** or **URLs** button.

It is possible to perform different actions on an archive or URL file.

 Retry processing file
Clicking this icon will trigger the Virex system to reprocess the archive or URL file.
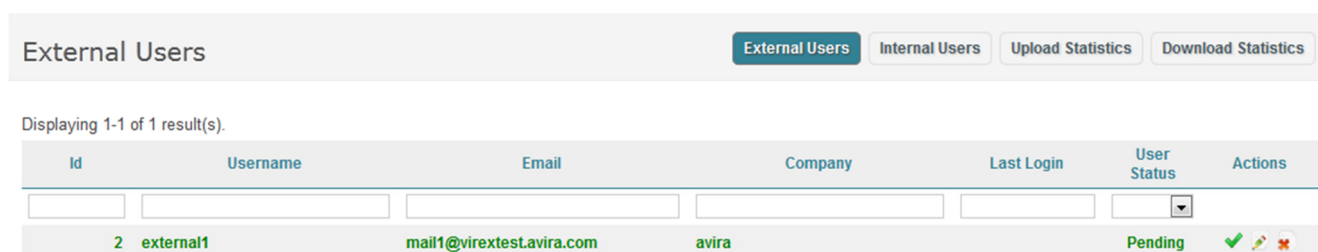
 Delete bogus archive/file
Clicking this icon will remove the uploaded archive or URL file from the system.

9.3 Administration

The **Administration** view provides information on external users, internal users, upload statistics and download statistics.

9.3.1 External Users

Clicking the **External Users** view in the **Administration** section will show the following table:

As you can see, the user status is set to "Pending," since the account is waiting for confirmation.
This view offers three actions for an external user.

 Enable user
Clicking this icon will activate the user account with rights to download daily and monthly collections by default.

 View/edit user details
Clicking this icon will open the **User details** page. You can define specific rights and sharing dates in this overview.

Delete account

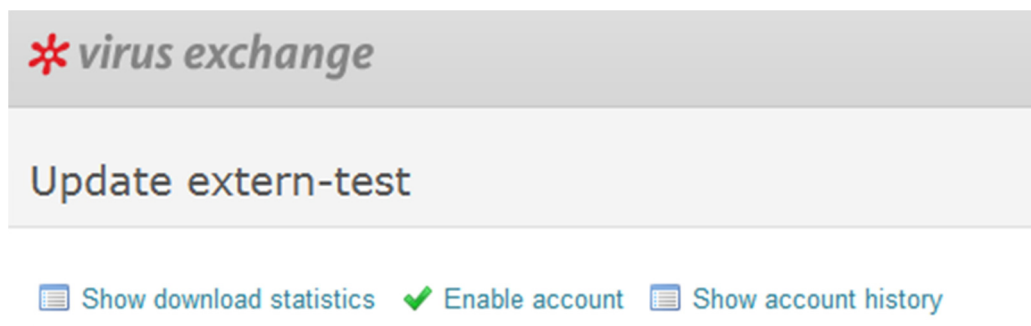Clicking this icon will remove the user account.

9.3.2 View/Edit User Details

Clicking the **View/Edit** icon opens a new page with all user details.

You are able to:

- Change the PGP key
- Change password
- Show download statistics
- Enable account (if status is pending)
- Show account history
- Change user rights
- Set a limitation date

Download statistics

The user download statistics page shows the last requested file lists as well as last downloaded files.
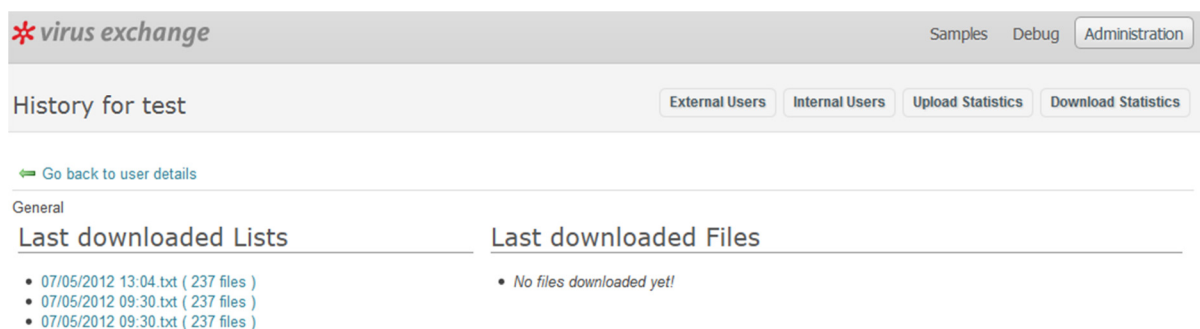
Enable account

Clicking this link enables the account for downloading samples from the Virex system.

Account history

The account history shows an archive of activities for an account. Events such as "Account created" or "Email validated" are displayed in this overview.

9.3.3   User Rights

Access is separated into four independent user rights.

1. **Daily**
   The user is able to download samples with status **daily**.

2. **Monthly**
   The user is able to download samples with status **monthly**.

3. **Clean**
   The user is able to download samples uploaded to the clean folder. The **clean** right must be combined with one or more of the other rights (according to the frequency at which you want to share clean samples).

4. **URLs**
   The user is able to request malware URLs from the Virex system.

Limitation date
The limitation date marks the beginning of the time frame in which a user can request samples from your server. This value is set to the registration date by default. If you want the user to have access to a higher of lower number of samples, you can change the limitation date to another date.

All changes (except enable account) have to be confirmed by pressing the **Save Changes** button.

9.3.4 Internal Users

An internal user in the Virex system has the same rights as the system administrator. Each internal user is able to create new internal users, enable/change external users and generate statistics.

To create a new internal user, go to the **Internal Users** view and click **Add a new user**.

Enter the new user's account details.

Checking/Un-checking the **Enabled** checkbox enables or disables the user.

9.3.5 Notifications

There are two types of notifications a user can receive.

Errors
If a user checks this box, he will receive an email notification if an error occurs in the Virex system.

New Account Request
If a user checks this box, he will receive an email notification when an external user has requested a new account.

After pressing the **Create** button, the new internal user will receive an email with an 8-digit generated password.

9.3.6 Statistics

The Virex system offers several statistics for internal users. Statistics are accessible via the **Administration** view.
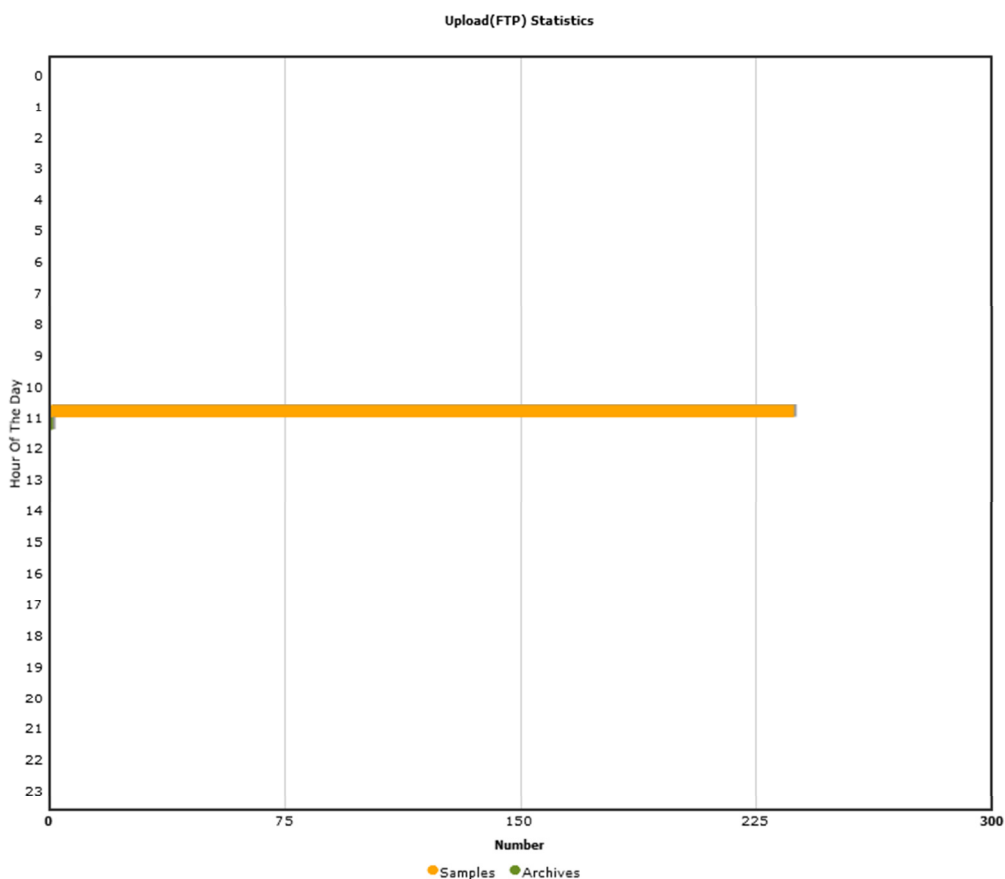
Upload Statistics

The **Upload Statistics** view provides statistics for archives/files uploaded to the Virex system. It's possible to generate statistics for:

- Number of files uploaded
- Average sample size
- Average archive size
- Total file size

It's possible to restrict the statistics to a defined timeframe and group them by hour, day, week or month.

A statistic for uploaded files on a specific day, grouped by hour could look like this:

Download Statistics

The **Download Statistics** view provides statistics for files downloaded by external users. It's possible to generate statistics on:

- Number of files
- File size (traffic)

Statistics can be limited to a defined timeframe and grouped by hour, day, week, month or user. Statistics for a specific user can be displayed by selecting the user in the **User** dropdown menu.