GTTA Workstation Setup manual

Workstation Installation & Configuration Help

General

This document describes the installation & configuration process of GTTA Workstation.

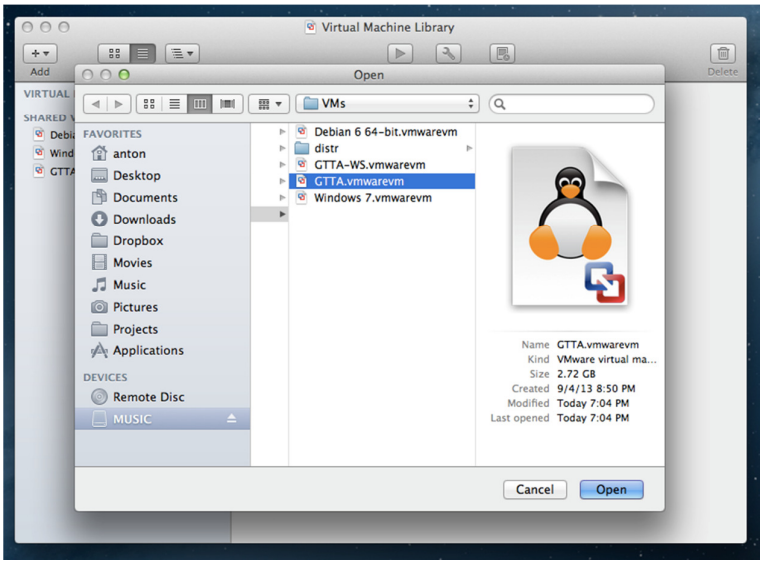
Prerequisites

In order to successfully install and use GTTA Workstation you should have the following:

1. VMware virtualization software – VMware Workstation, VMware Player or VMware Fusion.
2. GTTA Workstation distributive – archived virtual machine image for VMware (file named gtta-1.0.zip – the version number may differ in your case).

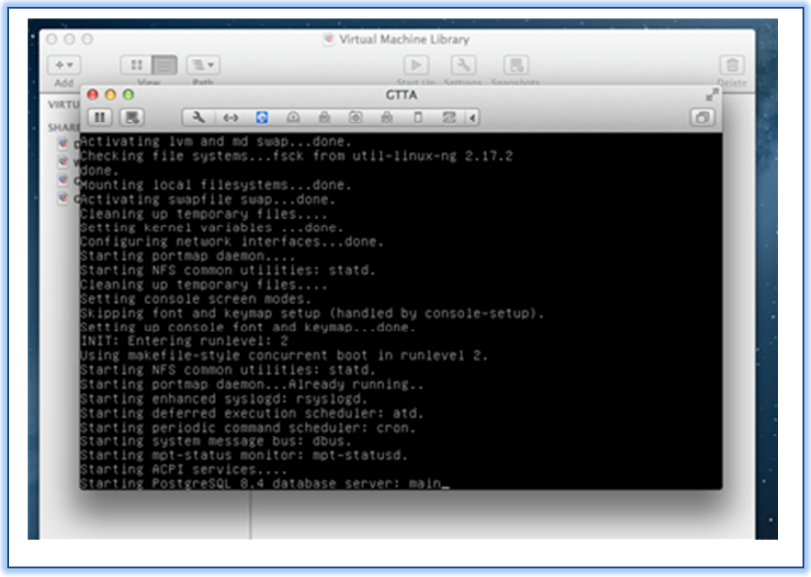
Installation

1. Extract the virtual machine image from the archive. Make sure that you have enough space on your drive – the extracted virtual machine occupies around 3 Gb of disk space. After you extract the archive, you will see a GTTA.vmwarevm folder that contains the virtual machine and all required files.
2. Open your VMware virtualization software.
3. Go to "File" - "Open" menu item – there you will see a file open dialog. Now find the extracted virtual machine image and press "Open". If you're on Windows or Linux, then you should open the GTTA.vmwarevm/GTTA.vmx file. If you're using Mac OS, then the extracted image will look like a single file and you should just choose GTTA.vmwarevm and open it. VMware Workstation will add this virtual machine to your VMware library.



4. By default the virtual machine is configured to use the bridged networking mode. If your host machine is connected to a public network, then you have to reconfigure it to use NAT. You can find how to do this in the VMware software manual. Make sure that you do this before booting the system for the first time.
5. Now choose the virtual machine in your library and press "Play" button to start the machine. GTTA Workstation will start booting.
6. After a while the system will start a GTTA configuration script – it will ask you to enter some settings that are required to operate in your environment. The configuration script will pass through the following steps:

- **Network Configuration**. On this step you should configure the system so it will be accessible from all clients that should have access to this GTTA Workstation instance. There are 2 options that you can choose. In order to choose the selected option, press the number in front of this option and press "Enter". You have the following options:



A) ***Manual Network Configuration*** – use this if you have no DHCP server in your network. If you will choose this, you will have to enter the workstation IP address, network mask and gateway IP address. Please make sure that you assign an IP address that is in the same subnet of your current network. For example, your physical computer's address could be 192.168.1.9, your router address could be 192.168.1.1 and you have no DHCP in the network. So you should enter these settings:

- IP address – 192.168.1.100
- Network mask – 255.255.255.0
- Gateway address – 192.168.1.1

  By default the system's address is 192.168.1.100, so if you are in the same subnet and this IP address is free, you can leave the default settings by pressing "Enter" on the corresponding fields.

  Please note, that if you are using NAT networking mode, then your NAT network will differ from the one that your physical computer is connected to. Usually, VMware's NAT network is 192.168.70.0/24 (with 192.168.70.1 assigned to the host computer), but your settings may be different. Please refer to VMware software manual for more information.

B) **DHCP Configuration** – use this if you have a DHCP server that will assign an IP address for your workstation automatically. Also if you are using NAT networking mode for your virtual machine, you may use this even if there is no DHCP server in your network, since

VMware software provides its own DHCP server for NAT connections.

After you choose this option, the system will attempt to obtain an IP address and if it will succeed, you will see a new address on the screen.

- **Domain Configuration**. On this step you should set the system domain name that will be used when you access your GTTA Workstation through the web browser. You may choose any domain name that you wish. The default domain name is gtta, you may leave it as it is.

  After you set a desired domain name, you should add a corresponding record to a DNS server within your network. If you have no DNS server, then you will need to add a domain record to the hosts file. This file's path is:

  a. Windows - C:\Windows\system32\drivers\etc\hosts
  b. Unix-like systems (Linux, Mac OS X, etc.) - /etc/hosts

- **Adding Administrative Account**. On this step the system will create an admin account for GTTA Workstation. It will ask you to enter a desired email & password for this account.

- **Root Certificate Generation**. The system won't need any actions on your side on this step – it will just silently generate the root certificate for user client-side certificates. These certificates can be used when you log in to the system, as an additional security measure.

7. After configuration process is complete, you will see a usual Linux login prompt. That means, that the system is booted up and ready to go.

8. Open your browser and type in the following URL: https://gtta/ (the domain name may differ, depending on your settings provided during the system configuration). You will see a warning about invalid SSL certificate. Ignore that warning and proceed to the URL

9. Use your admin login & password to enter the system.

10. Go to the "System" -> "Settings" menu and enter Workstation ID and Workstation Key there. This step is required to be able to receive and install software updates.

11. Now your system is ready to use.

Virtual Machine Configuration

You may change the virtual machine configuration anytime you wish by using GTTA configuration utility. This utility allows you to do the following:

- Configure network
- Change domain settings

- Add new admin account

There are 2 ways to configure your virtual machine:

1. Every time when you boot up your virtual machine, the system will start a GTTA configuration utility. It will allow you to change the system settings even if you can't access GTTA through the network. If you will not choose any configuration option within 10 seconds, the system will continue the normal booting process.
2. When the system is running, you can connect to it via SSH using user gtta and private RSA key (file named gtta-ssh or gtta-ssh.ppk). The system will launch the configuration utility immediately after you connect to it via SSH.

   If you are using Linux or Mac OS, then you can use the standard command-line client OpenSSH. The command in terminal will look like this:

   ssh –i /path/to/gtta-ssh gtta@*domain*

   Here *domain* stands for your configured domain name.

   If you are using Windows, then you may use the following SSH clients (name in bold means that the software is free):

   - **PuTTY** - http://www.chiark.greenend.org.uk/~sgtatham/putty/
     This software uses its own format for private keys, so you will need to use a key named gtta-ssh.ppk instead of gtta-ssh.
   - **TTY Emulator** - http://www.ttyemulator.com/
   - Private Shell – http://privateshell.com
   - ZOC - http://www.emtec.com/zoc/
   - eSSH - http://www.ecodesoftware.com/products/esh.html

   You can use any software listed above. Please specify the following settings when connecting to GTTA via SSH:

   - Hostname – the one you specified during the system configuration
   - Port – 22
   - Username – gtta
   - Authentication Method – Public Key
   - Private Key File – gtta-ssh (or gtta-ssh.ppk for PuTTY) with the following Key

     ssh-rsa
     AAAAB3NzaC1yc2EAAAADAQABAAABAQCbVY8l9HX7TreSTi9jxQxzm9vt0VcDUfWlNE/4XmRXf
     Fbc/rEP7Ip9wCD7AM2pkSogs5YS5sgNOvCJcXOTtkc52hzNXxu+y+WsXptEywphrKtmok4R1w4
     WYAgctEwVnvprDBNuF4tsmOYgm+D77Up8iTbHji7XnjBH6FvsX0fZhVyZ4Sxl9SL5lqXWtpEfGh1
     vWu7aS3+zFIjeCU4tEaqF/yIYypcC3VpG0WmL+VINx8S/krkEys9IBkJBx0EfmhGqORlzEF2uIyqxD
     aVH/2Y/7rLfxRDyN+c0nopmtUnJB2yOufV07K0dlx3/UYB09tq1teidnXtyNUsYH5nCv+wb
     gtta@gtta

Manual Installation

You can install GTTA manually to a Linux-powered host. This manual describes how to install GTTA to a Debian 6 (Squeeze) OS, but any modern Linux distribution should work. If you will choose some other distribution, you may need to use different package installation program and package names. Please refer to that distribution documentation for more information.

Please note, that in order to install the system using this way, you may need some basic Linux command-line skills and a root shell access to your server.

Software Prerequisites

GTTA has the following software prerequisites (Debian package names are in parentheses):

- Operating System: any modern Linux. Debian-based distributions are preferred.
- Database Server: PostgreSQL 8.1 or newer (*postgresql*)
- Web Server: Apache 2.2 or newer (*apache2*)
- Apache module for PHP (*libapache2-mod-php5*)
- PHP 5.2 or newer (*php5-cli*)
- PHP modules:
  - GD (*php5-gd*)
  - PgSQL (*php5-pgsql*)
- Python 2.5 or newer (*python*)
- Python modules:
  - Pip (*python-pip*)
  - LXML (*python-lxml*)
  - DNSPython 1.10 or newer (the version in Debian 6 repository is too old, install using pip by issuing the following command: pip install dnspython).
- Perl 5.8 or newer
- Perl modules:
  - Net::SSL (*libnet-ssleay-perl*, *libcrypt-ssleay-perl*)
  - XML::Simple (*libxml-simple-perl*)
  - Class::Accessor (*libclass-accessor-perl*)
  - Class::Data::Inheritable (*libclass-data-inheritable-perl*)
  - JSON::Any (*libjson-any-perl*)
  - LWP (*libwww-perl*)
  - Digest::MD5 (*libdigest-perl*)
  - Net::DNS (*libnet-dns-perl*)
  - Net::SSH2 (*libnet-ssh2-perl*)
  - Net::CIDR (*libnet-cidr-perl*)
  - Net::Whois::Raw (*libnet-whois-raw-perl*)
  - REST::Google (not available through Debian 6 repository, install using CPAN by issuing the following command: cpan REST::Google)
  - Net::Whois::IANA (install using CPAN by the following command: cpan Net::Whois::IANA)
- Nmap (*nmap*)
- TCP Traceroute (*tcptraceroute*)

To install all prerequisites you may issue the following commands on Debian system (you can just copy & paste them into your *root* terminal session):

- apt-get install apache2 libapache2-mod-php5 php5-cli postgresql php5-gd php5-pgsql python python-pip python-lxml libnet-ssleay-perl libcrypt-ssleay-perl libxml-simple-perl libclass-accessor-perl libclass-data-inheritable-perl libjson-any-perl libwww-perl libdigest-perl libnet-dns-perl libnet-ssh2-perl libnet-cidr-perl libnet-whois-raw-perl nmap tcptraceroute
- pip install dnspython
- cpan REST::Google
- cpan Net::Whois::IANA

If the commands above will complete successfully without displaying any errors, please proceed to the next step.

Uploading Files

Please follow these steps to upload GTTA files to your server:

1. Upload the system source directory gtta/ to the /opt/ directory on your server
2. Open a *root* terminal on your server
3. Go to the /opt/ directory on your server. You should see the gtta directory, that contains 2 subdirectories – gtta/scripts and gtta/web. The first subdirectory contains automated check scripts and the second – web GUI files.
4. Remove the uploaded archive file
5. Set "*readable and writable by all*" permissions (*777*) for the following directories (use chmod command):

- gtta/web/protected/runtime
- gtta/web/files/attachments
- gtta/web/files/automation

Database Server Configuration

Please follow these steps to set up your database server:

1. Open a *root* terminal on your server
2. Change current user to *postgres* using su command: su postgres
3. Start a PostgreSQL command shell: psql
4. Create a new user named *gtta* with password *123* (of course, you may use any other password, but in this case you will need to change this password in system configuration files – see the explanation below):
   create user gtta with password '123';
5. Create a new database named *gtta*:
   create database gtta;
6. Quit from PostgreSQL command shell
7. Exit from *postgres* user command shell and switch back to *root*
8. Open PostgreSQL Host Based Authentication configuration file. Its location depends on Linux distribution and PostgreSQL version. If you use Debian 6 and PostgreSQL 8.4, the file is located here:
   /etc/postgresql/8.4/main/pg_hba.conf

9. Allow password-based authentication for all local connection by addint the following line to the file:
   local all all password
10. Go to /opt/gtta/web/protected/data directory
11. Import a database dump located in database.sql file into your *gtta* database by issuing the following command:
    psql –U gtta gtta < database.sql

If you won't see any errors on this stage, please proceed to the next step.

Web Server Configuration

Please follow these steps to set up your web server:

1. Open a root terminal on your server
2. Create a new directory: /etc/apache2/ssl
3. Change your current directory to the newly created one
4. Create a self-signed SSL certificate for GTTA:

a. Create your RSA private key:

```
openssl genrsa -des3 -out gtta.key 1024
```

b. Generate a certificate signing request file:

```
openssl req -new -key gtta.key -out gtta.csr
```

c. Remove passphrase from private key:

```
cp gtta.key gtta.key.orig
openssl rsa -in gtta.key.orig -out gtta.key
```

d. Generate a self-signed certificate:

```
openssl x509 -req -days 365 -in gtta.csr -signkey gtta.key -out gtta.crt
```

5. Enable *rewrite* and *ssl* Apache modules by executing the following command:
   a2enmod rewrite ssl
6. Go to /etc/apache2/sites-available directory
7. Create a new virtual host file named gtta with the following contents (change *gtta-domain-name.com* to your domain name, if any):

```
<VirtualHost *:80>
    ServerName gtta-domain-name.com
    ServerAdmin webmaster@localhost

    DocumentRoot /opt/gtta/web
    <Directory />
        Options FollowSymLinks
        AllowOverride All
    </Directory>
    <Directory /opt/gtta/web/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        Order allow,deny
        allow from all
    </Directory>
```

```
    ErrorLog ${APACHE_LOG_DIR}/error.log
    LogLevel warn

    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

8. Create a new virtual host file named gtta-ssl with the following contents (change *gtta-domain-name.com* to your domain name, if any):

```
<VirtualHost *:443>
    ServerName gtta-domain-name.com
    ServerAdmin webmaster@localhost

    SSLEngine On
    SSLCertificateFile /etc/apache2/ssl/gtta.crt
    SSLCertificateKeyFile /etc/apache2/ssl/gtta.key

    DocumentRoot /opt/gtta/web
    <Directory />
        Options FollowSymLinks
        AllowOverride All
    </Directory>
    <Directory /opt/gtta/web/>
        Options Indexes FollowSymLinks MultiViews
        AllowOverride All
        Order allow,deny
        allow from all
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    LogLevel warn

    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

9. Disable a default Apache website by issuing the following command: a2dissite default
10. Enable newly created virtual hosts: a2ensite gtta gtta-ssl
11. Restart Apache: /etc/init.d/apache2 restart

Web Interface Configuration

There are 2 configuration files that you might need to change:

1. /opt/gtta/web/protected/config/main.php – main configuration file has the following settings:
    - 'db' – database settings:

- 'connectionString' – specifies the database host (host=), port (port=) and database name (dbname=)
- 'username' – database user name
- 'password' – database user password
- 'urlManager' => 'baseUrl' – base URL of the system
- 'entriesPerPage' – number of entries that will be displayed per page
- 'timeZone' – server time zone

2. /opt/gtta/web/protected/config/console.php – console configuration file that has the following settings:
   - 'db' – database settings (see database settings above)
   - 'interpreters' – interpreter paths and base directories

More than likely you won't need to change these files. After this step is done, try to open the software in your web browser. You should see a web interface and be able to log into the system using the following login details:

- Login: XXX (request info@netprotect.ch for pwd);
- Password: XXX (request info@netprotect.ch for pwd);

Background Workers Configuration

Please follow these steps to set up background workers:

1. Try to start some background workers manually – execute the following command from the command line:

```
cd /opt/gtta/web/protected && ./yiic vulntracker
```

You shouldn't see any errors on this stage. If everything works fine, please proceed to the next step.

2. Set up background tasks to run every minute by adding the following lines to a root crontab (crontab –e):

```
*/1 * * * *     cd /opt/gtta/web/protected && ./yiic automation
*/1 * * * *     cd /opt/gtta/web/protected && ./yiic email
*/1 * * * *     cd /opt/gtta/web/protected && ./yiic vulntracker
```

Now you're all set, the system is ready to use.