VIPole Corporate Server

for Windows Server

Installation and Configuration Manual

v.2.0, 2016

VIPole
www.vipole.com

SECURE AND ENCRYPTED MESSENGER
for secure communications and encrypted data storage

Windows ▪ Mac OS ▪ Linux ▪ Android ▪ iOS ▪ Enterprise solutions

Recommended server requirements for installing VIPole Corporate Server

- Windows Server 2008 R1 x64
- Multi-core processor (4 cores recommended)
- 16 Gb+ RAM
- 1Tb HDD (RAID1 or RAID10)

During VIPole Corporate Server installation, additional components installing is required:

- MongoDB , version 2.6
- Redis, version 2.6 or later
- Win64 OpenSSL v1.0.2d Light or later

Windows Firewall Settings

Check Windows Firewall settings. Turn off Windows Firewall or configure the settings to allow using the necessary ports. You can find the port list in VIPole server and relay server configuration files.

> **Note,** that there is a range of ports in relay.config file!

server.config:

```
# Server port
listen-port = 37210
# UDP port of SIP server
sip-server-port=5060
```

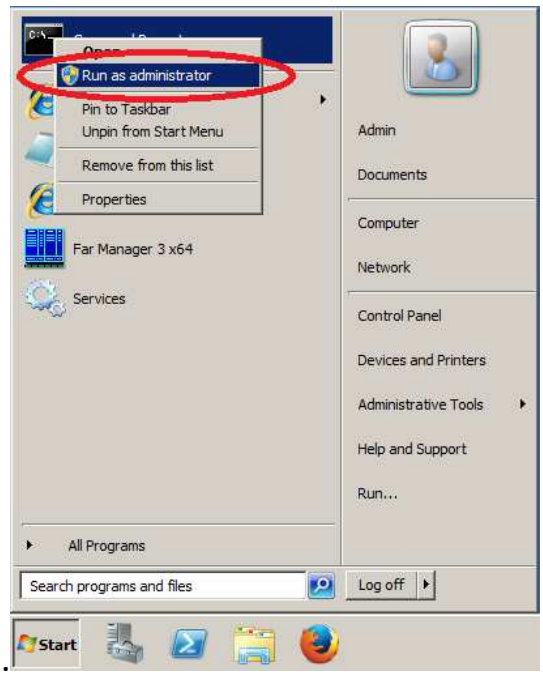
relay.config

```
# UDP ports range
# Minimum UDP port
min-port=3000
# Maximum UDP port
max-port=9000
```

server-auto.config

```
# Server port
listen-port = 37212
```

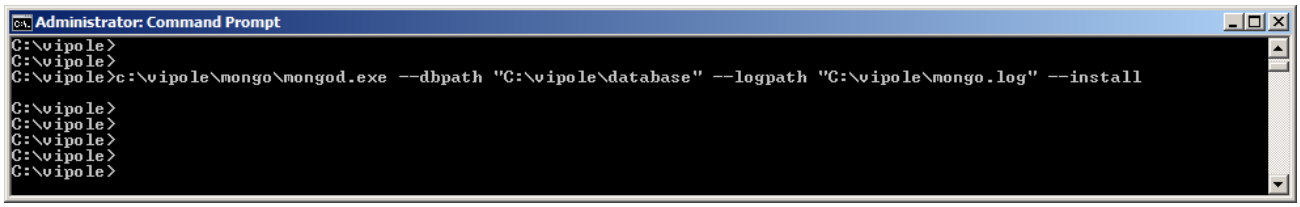
All commands **`in bold monospaced type`** shall be run in the command prompt. To open the command prompt, run **`cmd.exe`** as administrator.



Some commands are too long and are therefore split into several lines.

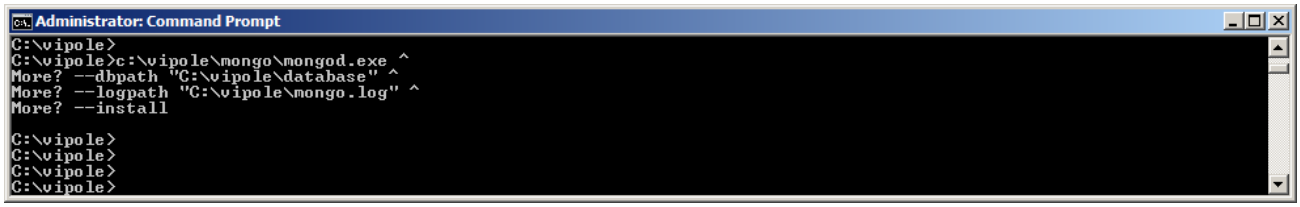
When there is the **^** symbol in the end of the line, Windows command line interpreter considers the command to be continuing on the next line. For example, the command

```
c:\vipole\mongo\mongod.exe --dbpath "C:\vipole\database" --
logpath "C:\ vipole \mongo.log" --install
```



can be entered in the following way

```
c:\vipole\mongo\mongod.exe ^
--dbpath "C:\vipole\database" ^
--logpath "C:\vipole\mongo.log" ^
--install
```



Command execution results are the same in both cases.

Installation

We will install VIPole Corporate Server to the c:\vipole folder

```
md c:\vipole
```

1. Install the necessary updates for Windows Server OS

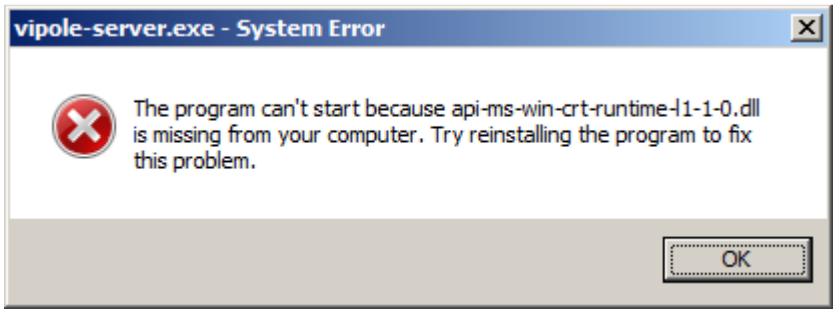
If you use Windows Server 2008 R2 x64, it is necessary to install the KB2999226 update for Windows Server 2008 R2 x64 Edition

https://www.microsoft.com/en-US/download/details.aspx?id=49062

For other Windows Server versions download and install Microsoft Visual C++ 2015 Redistributable Package.

https://www.microsoft.com/en-US/download/details.aspx?id=48145

If the necessary updates are not installed, the system error occurs:



2. Installing MongoDB, version 2.6

2.1. MongoDB at

https://fastdl.mongodb.org/win32/mongodb-win32-x86_64-2008plus-2.6.12.zip

2.2. Create a folder for the program

```
md c:\vipole\mongo
```

and for the database

```
md c:\vipole\database
```

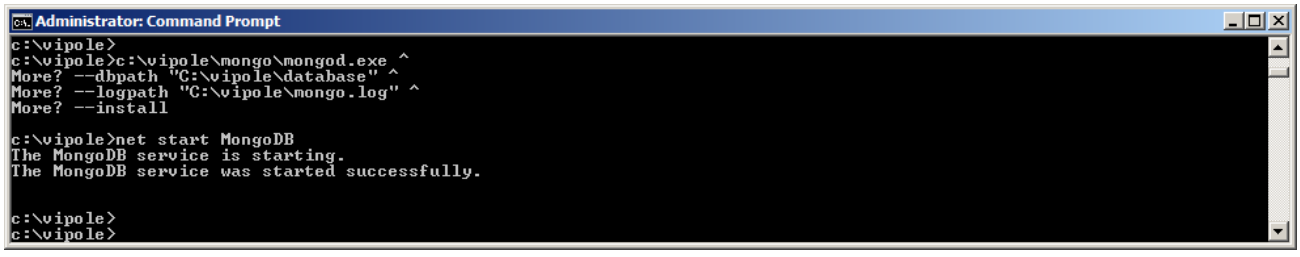
2.3. Unpack the archive **`bin\`** folder of the MongoDB archive to the folder **`c:\vipole\mongo`**

2.4. Install mongod as a service

```
c:\vipole\mongo\mongod.exe ^
--dbpath "C:\vipole\database" ^
--logpath "C:\vipole\mongo.log" ^
--install
```

2.5.Start mongo service by command

```
net start mongoDB
```



3. Redis 2.8 installation

3.1. Download Redis

https://github.com/MSOpenTech/redis/releases/download/win-2.8.2400/Redis-x64-2.8.2400.zip

3.2. Create Redis folder

```
md c:\vipole\redis
```

3.3. Unpack **Redis-x64-2.8.2400.zip** to folder **c:\vipole\redis**

3.4. Replace in file **c:\vipole\redis**\redis.windows-service.conf

the line

```
logfile "Logs/redis_log.txt"
```

with

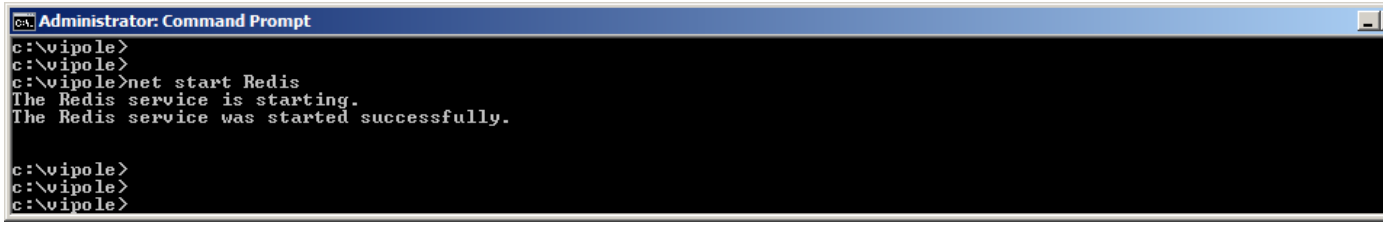
```
logfile "redis.log"
```

3.5. Install Redis as a service

```
c:\vipole\redis\redis-server ^
--service-install ^
c:\vipole\redis\redis.windows-service.conf ^
--loglevel verbose
```

Run Redis service by command

```
net start redis
```



4. Install VIPole Corporate Server software package

4.1. Create a folder for VIPole Corporate Server

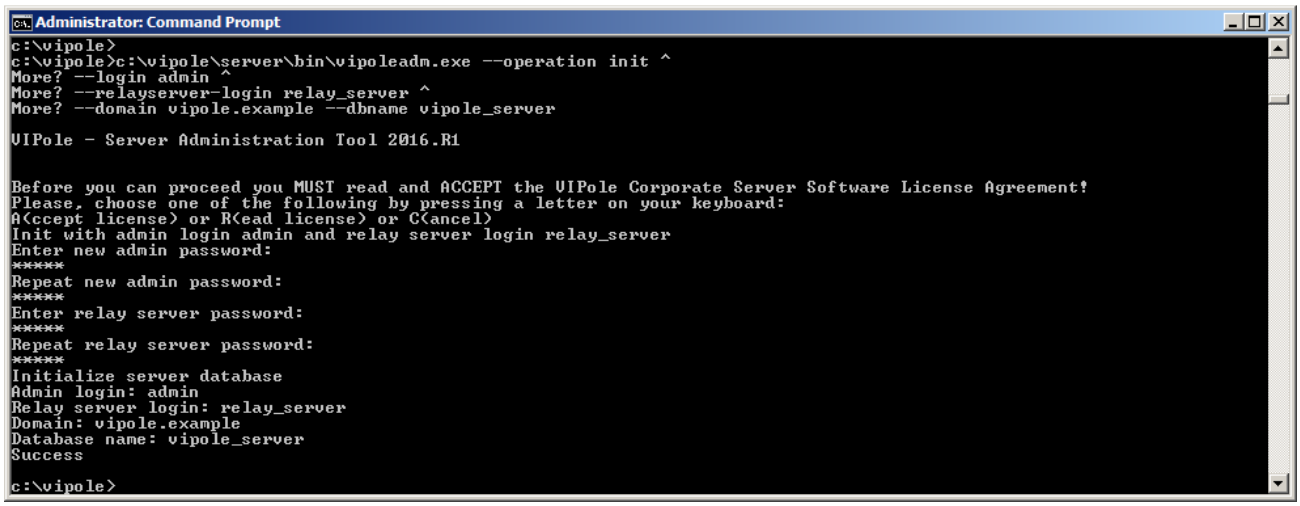
```
md c:\vipole\server
```

4.2. Unpack VIPole Corporate Server software package to `c:\vipole\server\`

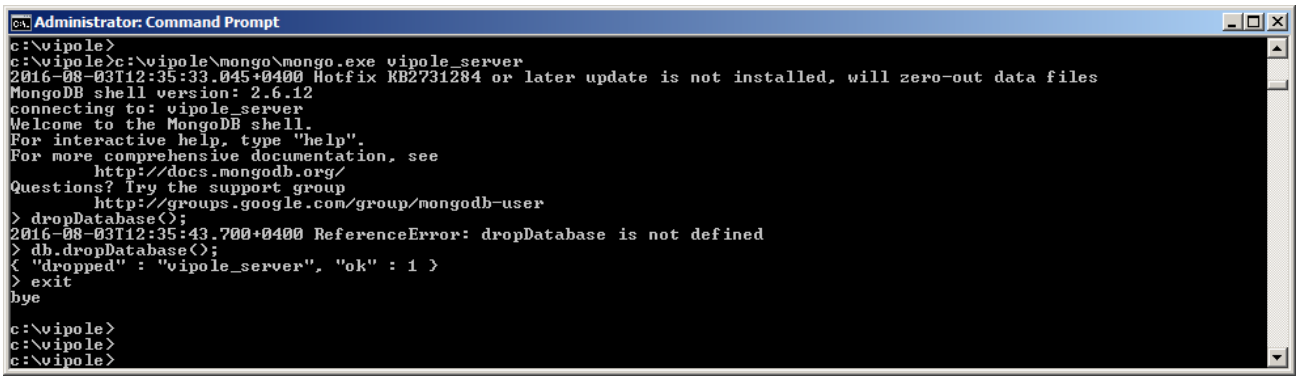
Note, that there are three folders in the archive – `\bin` , `\config` and `\locale`

4.3. Initialize the data base by creating accounts for the administrator and the relay server. Read and confirm the License Agreement. Then you need to set passwords for the created accounts.

```
c:\vipole\server\bin\vipoleadm.exe --operation init ^
--login admin ^
--relayserver-login relay_server ^
--domain vipole.example --dbname vipole_server
```



> If you decide to initialize the database again, you need to start Mongo with database name as a parameter, for example, that you specified in the dbname parameter in sec. 4.3.
>
> ```
> c:\vipole\mongo\mongo.exe <database_name>
> ```
>
> After Mongo welcome message, enter the command
>
> ```
> db.dropDatabase();
> ```
>
> and then
>
> ```
> exit
> ```



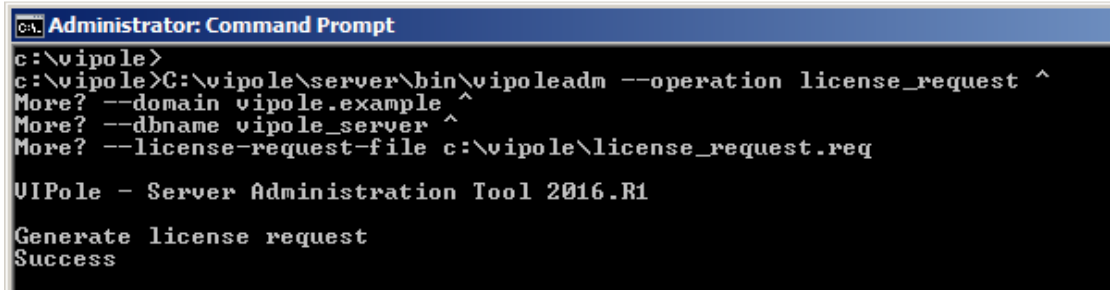
Note! During the database initialization, the unique identifier is changed, to which the license is assigned. Therefore, re-initialization is allowed **only before performing sec. 4.6.**

Re-initialization after the license request has been generated will lead to making the license invalid.

It will be impossible to restore it, and you will have to buy it again.

4.4. Now you need to generate a license request:

```
C:\vipole\server\bin\vipoleadm --operation license_request ^
--domain vipole.example ^
--dbname vipole_server ^
--license-request-file c:\vipole\license_request.req
```



Note! The license will be assigned to the initialized database.

The required parameters:

--operation license_request

--domain – your domain, specified in sec. 4.3

--dbname – database name, specified in sec. 4.3

--license-request-file – the pathname for storing license request. Note that the pathname should be written in Latin symbols and/or numbers.

4.5. **Send us a license request file via email to contact@vipole.com providing your company details or to your personal manager. As soon as we receive the license request file, we will send you back the license file.**

To add additional user licenses there is no need to send the license request again. All you need is to purchase additional user licenses and you will get a file with these new licenses.

4.6. When you get the license file, check its validity and look through the content:

```
c:\vipole\server\bin\vipoleadm --operation verify_license ^
--domain vipole.example --dbname vipole_server ^
--license-file vipole_license_C1000016D160803N051LID0000176.dat
```

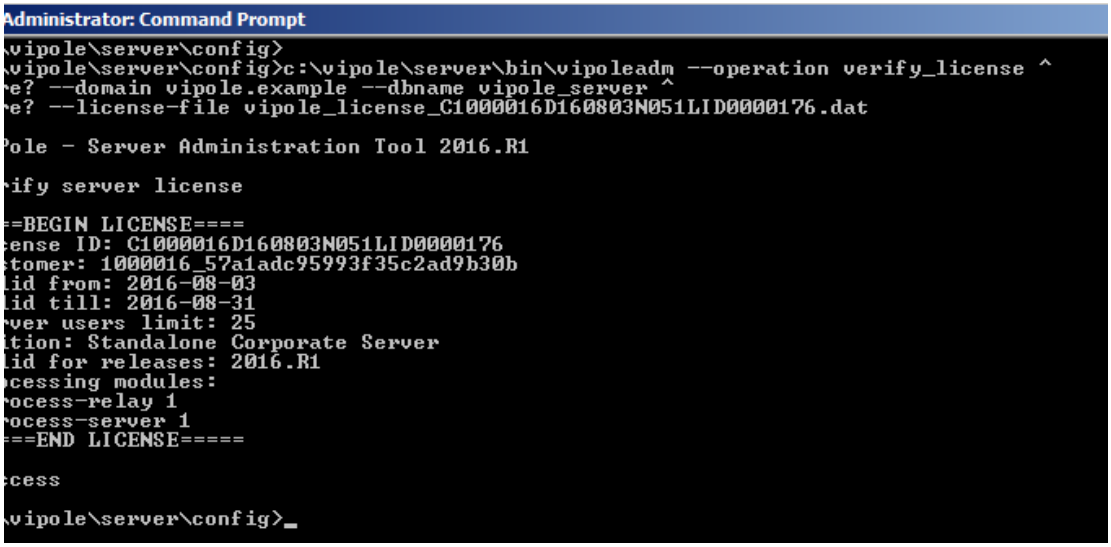
Mandatory parameters:

--domain – your domain, specified in sec. 4.3

--dbname – database name, specified in sec. 4.3

--operation verify_license

--license-file – the pathname for storing the license. Note that the pathname should be written in Latin symbols and/or numbers.



4.7. To activate the license run a command:

```
c:\vipole\server\bin\vipoleadm --operation activate_license ^
--domain vipole.example --dbname vipole_server ^
--license-file vipole_license_C1000016D160803N051LID0000176.dat
```

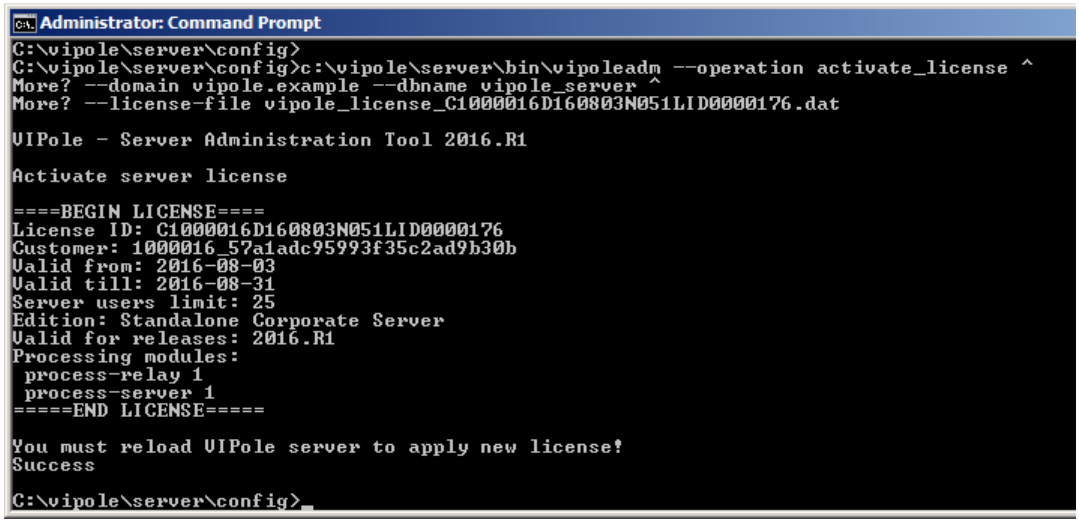
Mandatory parameters:

--operation activate_license

--domain – your domain, specified in sec. 4.3

--dbname – database name, specified in sec. 4.3

--license-file – the pathname for storing the license. Note that the pathname should be written in Latin symbols and/or numbers.



4.8. You can check the current status of the license packages at any time:

```
c:\vipole\server\bin\vipoleadm  --operation
print_server_license ^
--domain vipole.example --dbname vipole_server
```

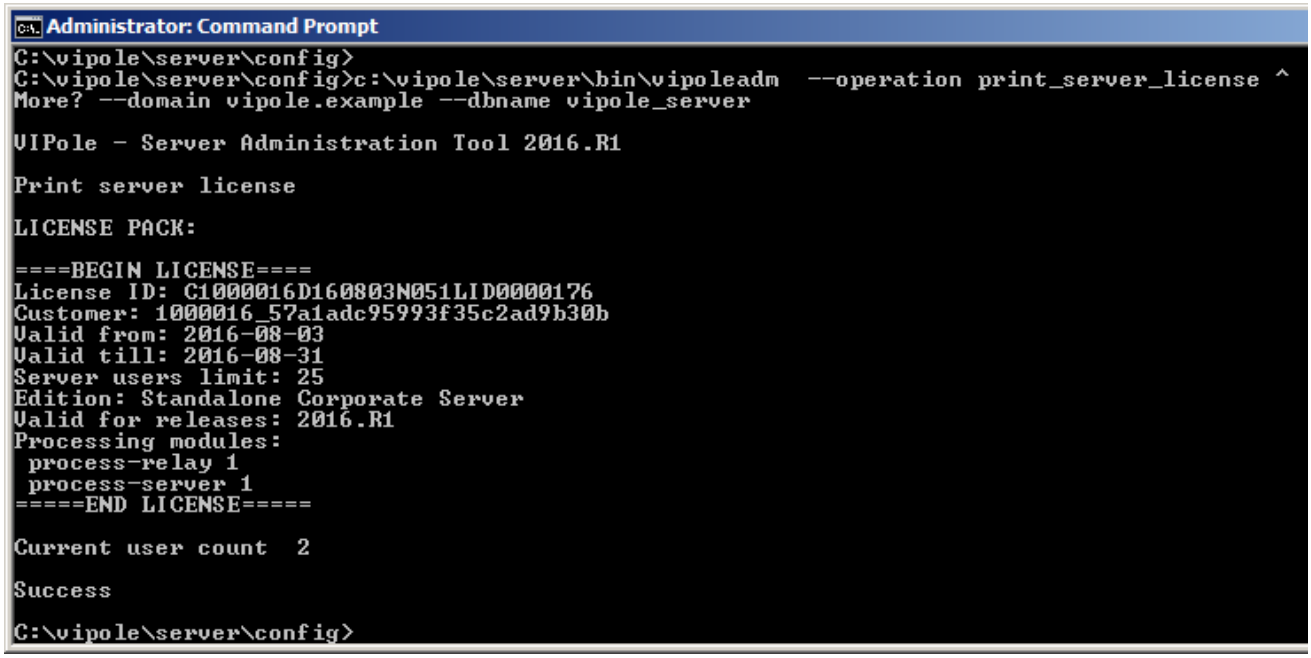
Mandatory parameters:

`--operation print_server_license`

`--domain` – your domain, specified in sec. 4.3

`--dbname` – database name, specified in sec. 4.3

If you have one license, you will see the package content. If you have several license packages, you will see the content of all packages, as well as the combined license, formed by combining all actual license packages as of the current date and server version.

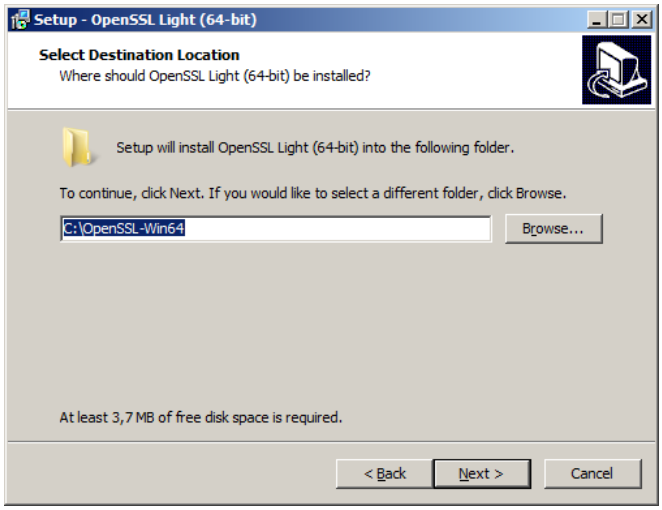


5. Generate server certificate using OpenSSL

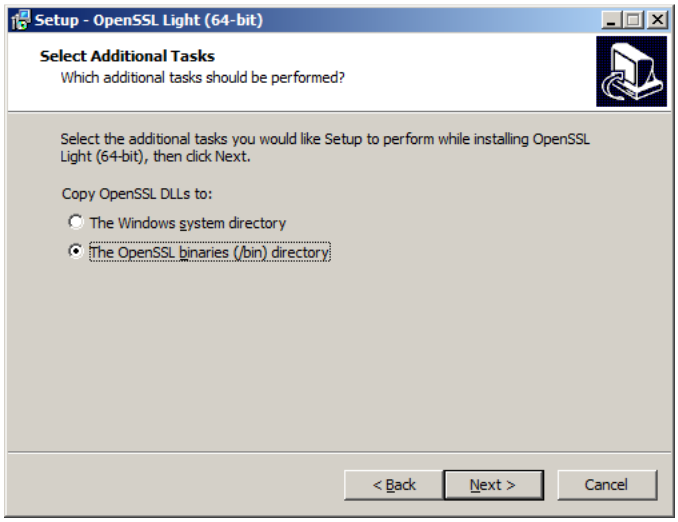
5.1. Download OpenSSL at http://slproweb.com/products/Win32OpenSSL.html

and install it. For example, Win64 OpenSSL v1.0.2h Light.

Install OpenSSL to the default folder **C:\OpenSSL-Win64\bin**



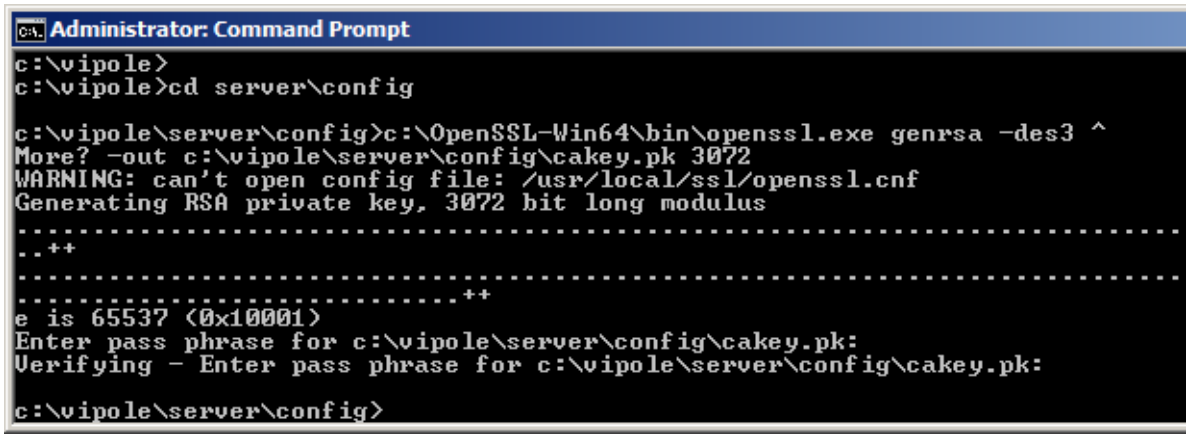
Copy «OpenSSL DLLs to binaries (/bin) directory»



5.2. Generate a private key

```
c:\OpenSSL-Win64\bin\openssl.exe genrsa -des3 ^
-out c:\vipole\server\config\cakey.pk 3072
```

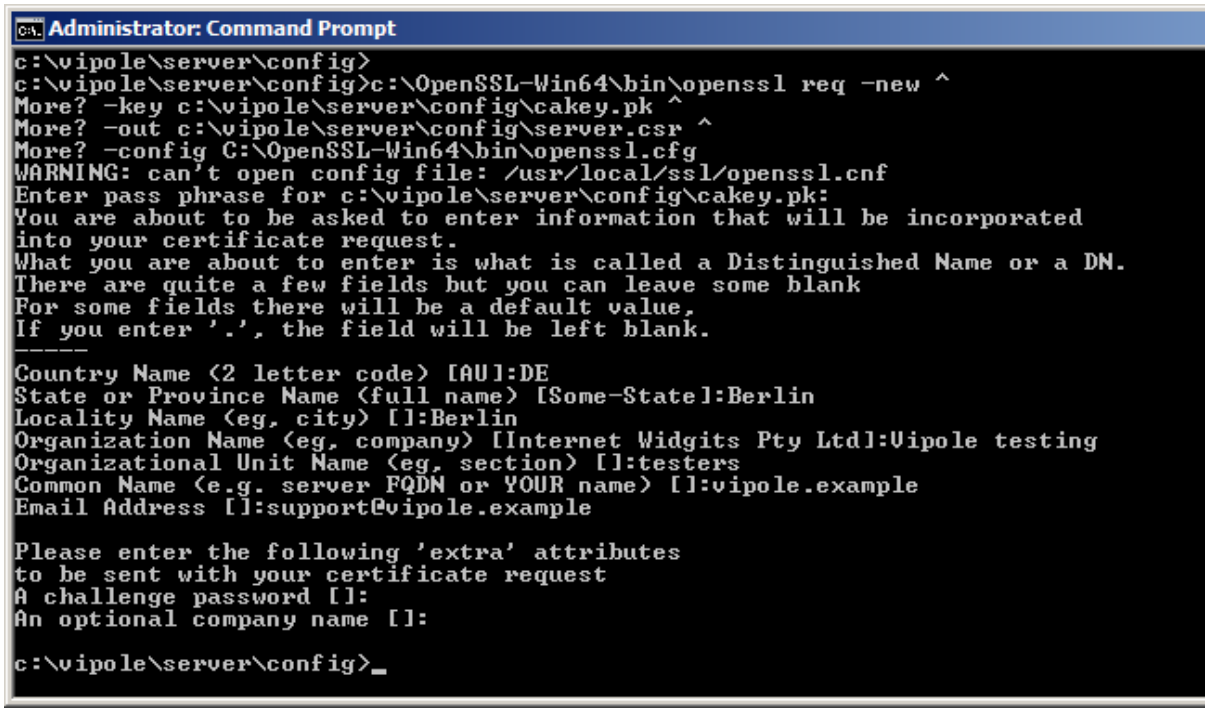
To the «Enter pass phrase for» request create and enter your password. It will later be used during the server configuration.



5.3.Generate a certificate request

```
c:\OpenSSL-Win64\bin\openssl req -new ^
-key c:\vipole\server\config\cakey.pk ^
-out c:\vipole\server\config\server.csr ^
-config C:\OpenSSL-Win64\bin\openssl.cfg
```

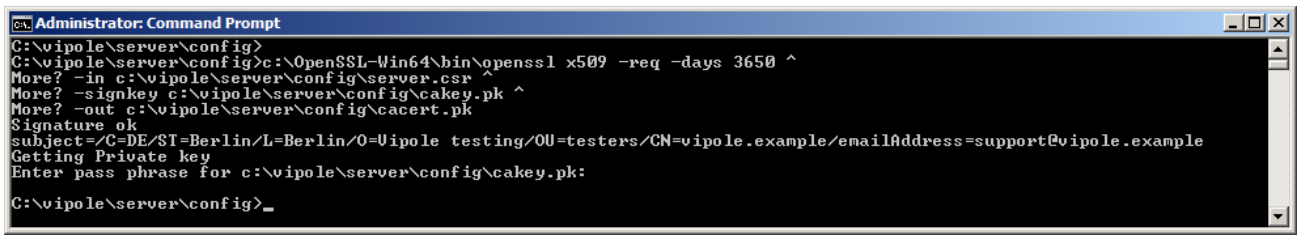
To the request «Enter pass phrase for», enter the password from sec. 5.2.



5.4. VIPole Corporate Server allows to use self-signed certificates:

```
c:\OpenSSL-Win64\bin\openssl x509 -req -days 3650 ^
-in c:\vipole\server\config\server.csr ^
-signkey c:\vipole\server\config\cakey.pk ^
-out c:\vipole\server\config\cacert.pk
```

To the request «Enter pass phrase for» enter the password from sec. 5.2.



6. Server configuration

Copy the contents of the file

c:\vipole\server\config\server.config.sample

to

c:\vipole\server\config\server.config

```
copy c:\vipole\server\config\server.config.sample ^
c:\vipole\server\config\server.config
```

Edit c:\vipole\server\config\server.config : you need to specify your server domain name, IP address, full path to certificate and private key, as well as the passphrase for the private key.

Enter the path to the private key, generated at sec. 5.2

```
private-key-file = c:\vipole\server\config\cakey.pk
```

Enter the passphrase that you created at sec. 5.2

```
private-key-file-passphrase = <passphrase>
```

Enter the path to the certificate, obtained at sec. 5.4

```
certificate-chain-file = c:\vipole\server\config\cacert.pk
```

Then you need to specify the IP address, where VIPole corporate server will accept connections. The 0.0.0.0 address means «all interfaces». You can also specify a particular IP-address of the Windows server external interface.

```
listen-address = 0.0.0.0
```

Enter the domain name, the same as in sec. 4.3

```
domain = example.com
```

If you have purchased a SIP module license, you need to set the connection parameters for the SIP server.

Enable SIP module

```
sip-enable=true
```

Enable setting the SIP account of the user at the admin panel

```
sip-enable-admin=true
```

Enter your SIP server address

```
sip-server-address = 192.168.1.65
```

Enter the UDP port number of the SIP server

```
sip-server-port=5060
```

Enter the actual VIPole server IP address that will be used for SIP server connections.

```
sip-local-address = 192.168.1.215
```

SIP phone domain name. It is the domain that will be added to the number (for example, +12345678@sip-to-phone.example.com, where sip-to-phone.example.com is the domain name).

You can also specify the IP-address of the SIP-server.

```
sip-phone-domain = 192.168.1.65
```

7. Media relay configuration

Copy the contents of the file

c:\vipole\server\config\relay.config.sample

to

c:\vipole\server\config\relay.config

```
copy c:\vipole\server\config\relay.config.sample ^
c:\vipole\server\config\relay.config
```

Edit c:\vipole\server\config\relay.config: you need to enter your login and password of the Relay Server account, public IP address and the full path to the server certificate.

The external IP-address is the one to which the clients will connect. It is usually the address of the Windows server external network interface. If you have installed the server for NAT and use port forwarding, the external NAT address should be indicated as external-listen-address

```
external-listen-address=10.10.1.180
```

The media relay login that is set by the option --relayserver-login in sec. 4.5 If you use several media relays, they need to use the same login.

```
login=relay_server
```

Enter the domain name, the same as in sec. 4.3

```
domain=vipole.example
```

The media relay password, set in sec. 4.5

```
passwd=<password >
```

The path to the certificate, obtained in sec. 5.4

```
certificate=c:\vipole\server\config\cacert.pk
```

8. **Start VIPole Server as a console application**

First run a command to verify that there are no errors in the configuration file:

```
c:\vipole\server\bin\vipole-server ^
--config c:\vipole\server\config\server.config
```

If there was not a command prompt within 30 seconds, it means that the server has successfully started. Interrupt its work by pressing CTRL+C.

Then run it in a separate window with the command:

```
start c:\vipole\server\bin\vipole-server ^
--config c:\vipole\server\config\server.config
```

9. **Start the media Relay Server as console application**

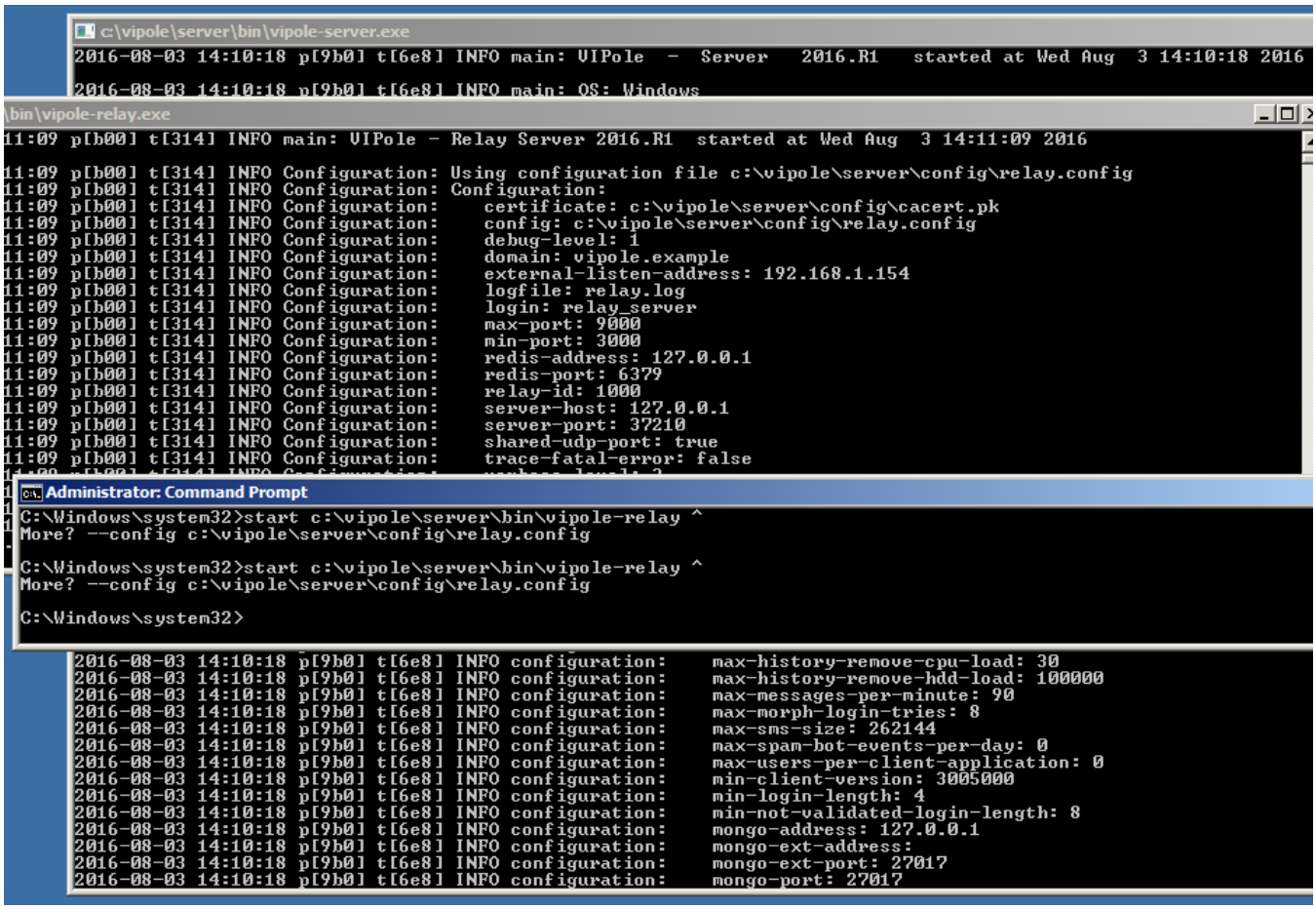
First run a command to verify that there are no errors in the configuration file:

```
c:\vipole\server\bin\vipole-relay ^
--config c:\vipole\server\config\relay.config
```

If there was not a command prompt within 30 seconds, it means that the server has successfully started. Interrupt its work by pressing CTRL+C.

Then run it in a separate window with the command:

```
start c:\vipole\server\bin\vipole-relay ^
--config c:\vipole\server\config\relay.config
```

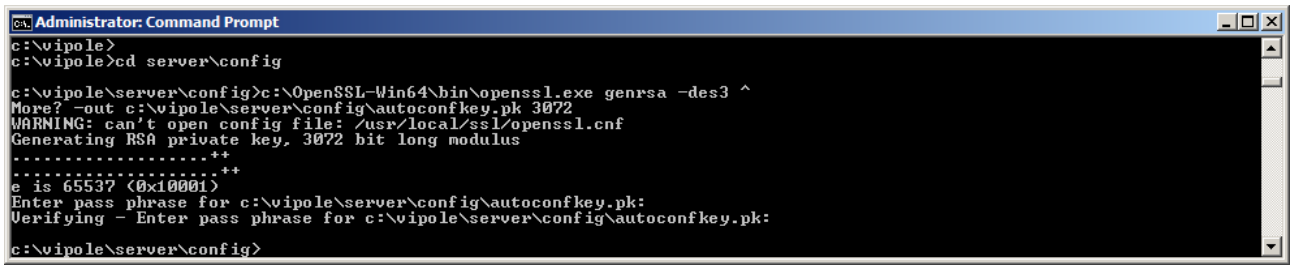


10. Configure the autoconfig server

The autoconfig server is designed for applying VIPole client connection settings automatically. Using the autoconfig server is not mandatory and its settings and run can be skipped.

10.1. Generate a private key for the autoconfig server

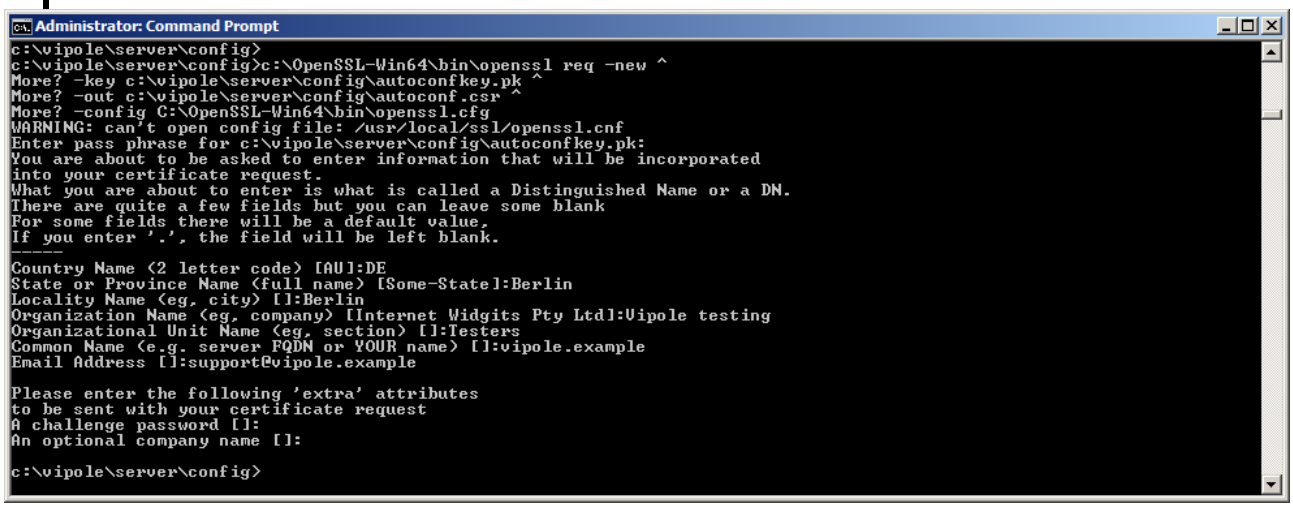
```
c:\OpenSSL-Win64\bin\openssl.exe genrsa -des3 ^
-out c:\vipole\server\config\autoconfkey.pk 3072
```



10.2. Generate a certificate request.

```
c:\OpenSSL-Win64\bin\openssl req -new ^
-key c:\vipole\server\config\autoconfkey.pk ^
-out c:\vipole\server\config\autoconf.csr ^
-config C:\OpenSSL-Win64\bin\openssl.cfg
```

> You **must** specify the FQDN when generating a certificate request



10.3. Send us the certificate request file via email to contact@vipole.com providing your company details or to your personal manager and you will receive a signed certificate. Only the signed certificate can be used for the autoconfig server.

10.4. **Setting the client autoconfiguration file**

Copy file content

`c:\vipole\server\config\client_autoconf.config.sample`

to

`c:\vipole\server\config\client_autoconf.config`

```
copy c:\vipole\server\config\client_autoconf.config.sample
^
c:\vipole\server\config\client_autoconf.config
```

Edit the client_autoconf.config file:

Enter the certificate file that you have received from us in sec. 10.3.

```
autoconf-sign-certificate-file=
c:\vipole\server\config\vipole_certificate.pem
```

Enter the private key for the autoconfig server, that you have received in sec.10.1.

```
autoconf-sign-private-key-file=
c:\vipole\server\config\autoconfkey.pk
```

Set 1 as a parameter value if you want the clients to enter access code for autoconfiguration.

```
autoconf-use-access-code=0
```

If you use the access code, set the it here

```
#autoconf-access-code=
```

Enter the VIPole server certificate file, that you have received in sec. 5.5

```
vipole-server-certificate-file=
c:\vipole\server\config\cacert.pk
```

The client_autoconf.config file contains the settings that are specific to your configuration and are transferred to the client program.

Enter the domain name or the IP-address of your server (the IP address must match the value of the parameter `external-listen-address`, set in sec.7)

```
vipole-server-host=10.10.1.180
```

VIPole server port number

```
vipole-server-port=37210
```

If you use SIP server, enter 1

```
sip-enable=0
```

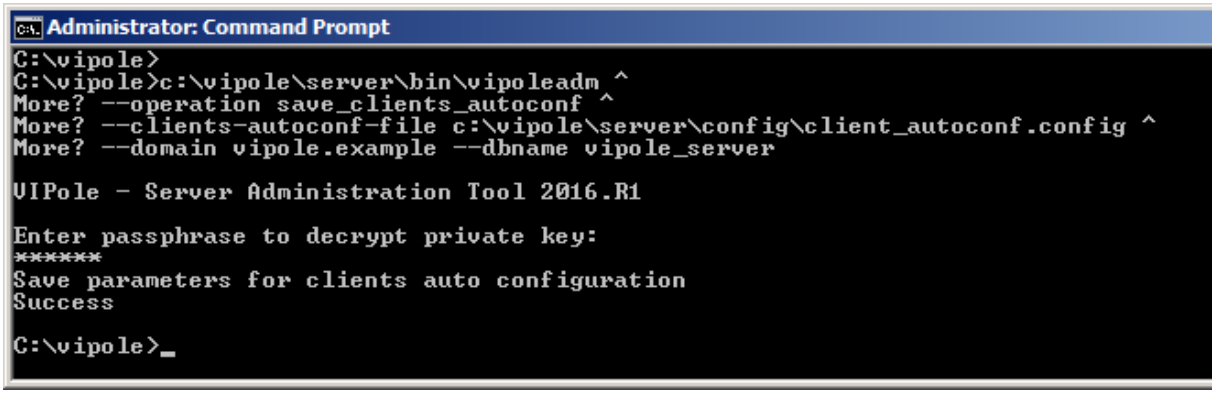
If you use E.123 numbers (the number starts with + , then goes the country code and the phone number, for example, +123456789), set the parameter value as 1. If there are no special dialing rules (for example, it is your local SIP station and you can use any numbers, e.g. 106) then set the parameter value as 0.

```
sip-strict-phone-number=1
```

10.5. Save the autoconfiguration settings to the database

```
c:\vipole\server\bin\vipoleadm ^
--operation save_clients_autoconf ^
--clients-autoconf-file
c:\vipole\server\config\client_autoconf.config ^
--domain vipole.example --dbname vipole_server
```

To the request «Enter passphrase to decrypt private key» enter the password from sec. 10.1



If you need to change autoconfiguration settings, edit the client_autoconf.config file and run vipoleadm again. After you save the autoconfiguration settings, you need to restart only the autoconfig server.

10.6. Configuring the autoconfig server

Copy the contents of the file c:\vipole\server\config\server.config.sample to c:\vipole\server\config\server-auto.config .

```
copy c:\vipole\server\config\ server-auto.config.sample  ^
c:\vipole\server\config\server-auto.config
```

Edit the file **server-auto.config:**

Enter the full path to the private key file that you have received in sec. 10.1

```
private-key-file = c:\vipole\server\config\autoconfkey.pk
```

Enter the password for the private key that you have received in sec. 10.1

```
private-key-file-passphrase = secret_passphrase
```

Enter the full path to the certificate file, that your have received back in sec. 10.3

```
certificate-chain-file =
c:\vipole\server\config\vipole_certificate.pem
```

Enter your VIPole server domain

```
domain = example.com
```

Enter the IP address of the autoconfig server. This is the IP address, where VIPole corporate server will accept connections. The 0.0.0.0 address means «all interfaces». You can also specify a particular IP-address of the Windows server external interface.

```
listen-address = 0.0.0.0
```

Enter autoconfig server port

```
listen-port = 37212
```

The following settings should match the VIPole server settings:

Enter the MongoDB server IP address

```
mongo-address = 127.0.0.1
```

MongoDB server TCP port

```
mongo-port = 27017
```

Database name

```
dbname = vipole_server
```

10.7. Start autoconfig server as a console application:

First run a command to verify that there are no errors in the configuration file:

```
c:\vipole\server\bin\vipole-server --autoconf ^
--config c:\vipole\server\config\server-auto.config
```

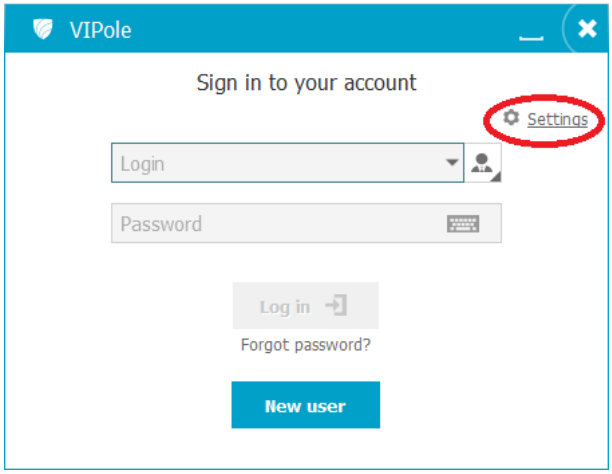
If there was not a command prompt within 30 seconds, it means that the server has successfully started. Interrupt its work by pressing CTRL+C.

Then start it in a separate window with the command:

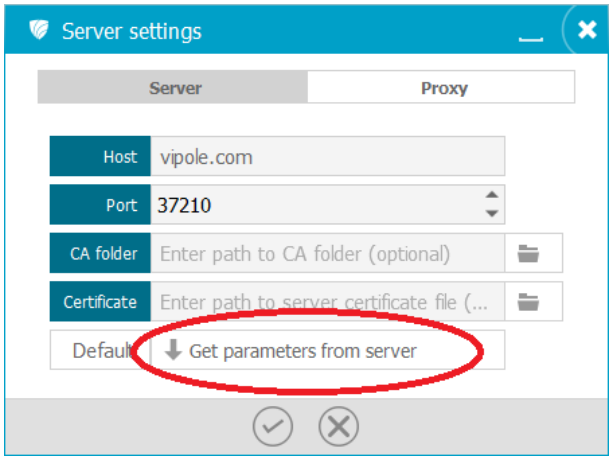
```
start c:\vipole\server\bin\vipole-server --autoconf ^
--config c:\vipole\server\config\server-auto.config
```

Check if it runs correctly by configuring the client as described in the next section.

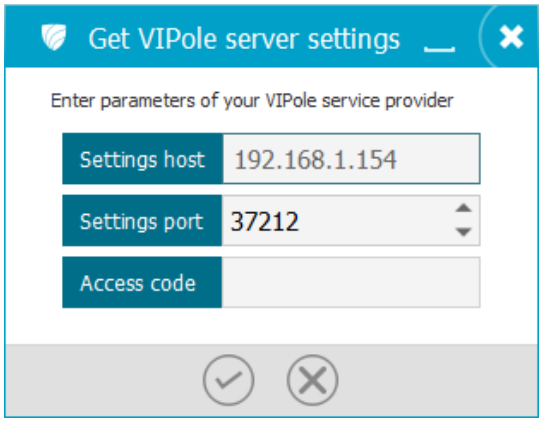
10.8. To use autoconfiguration, when starting the application click on Settings before entering VIPole ID (Login).

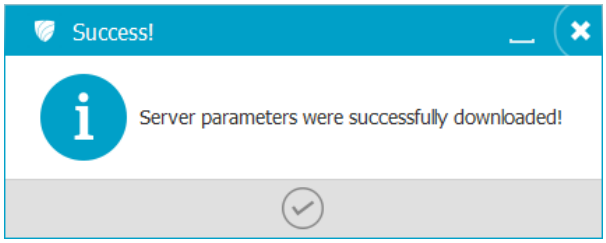


Click on «Get parameters from server»:



In the opened window, enter the autoconfig server IP address and the port number. Then enter the access code if you have set it.





When you press the ✓ button, VIPole client application gets all network settings from the server automatically.

11. Setting servers running as Windows services

When you've checked that VIPole Server and Relay Server start and work correctly, you can launch them as services. You will need the NSSM program for this. It helps to create services and make service settings. You can use any other application that helps to create services.

There is an example of service creation in install-services.cmd file.

11.1. First, stop the **`vipole-server`** and **`vipole-relay`** servers, that were started from the console with the **start** command. One by one select the windows: **`vipole-server`**, then **`vipole-relay`** and press CTRL+C in each of them.

11.2. Then configure the services using the example file.

- See the example of service creation in the install-services.cmd file.
- See the example of running the services in the start-services.cmd file.
- See the example of removing services in remove-services.cmd file.

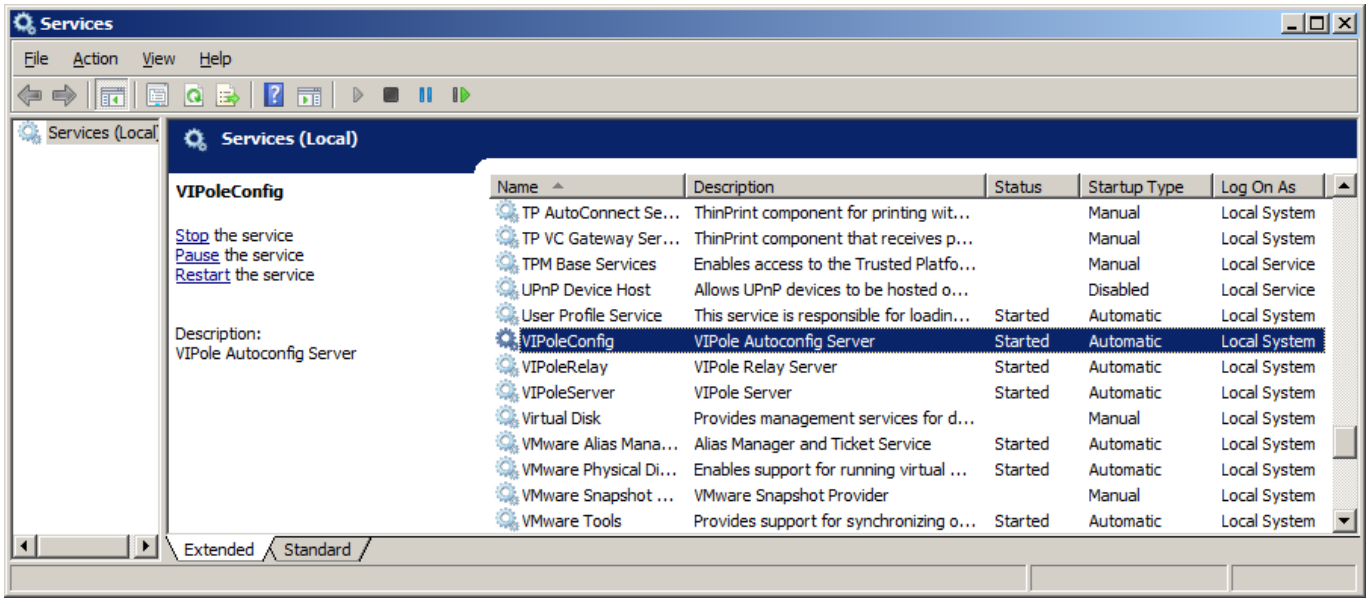
To start and stop services, you can also use the standard Windows commands **net start** and **net stop**, and the «Services» program of Windows management console.

Start all services:

```
net start VipoleServer
net start VipoleRelay
net start VipoleConfig
```

Stop all services:

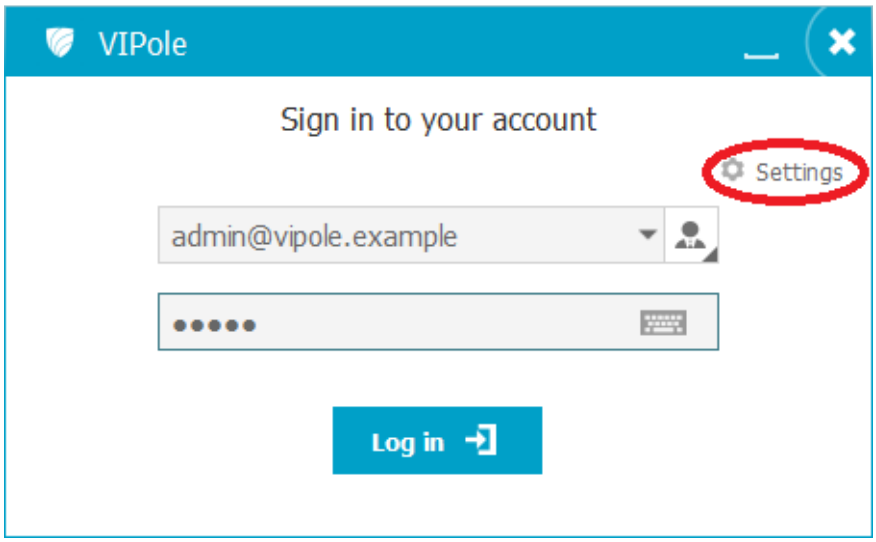
```
net start VipoleConfig
net start VipoleRelay
net start VipoleServer
```



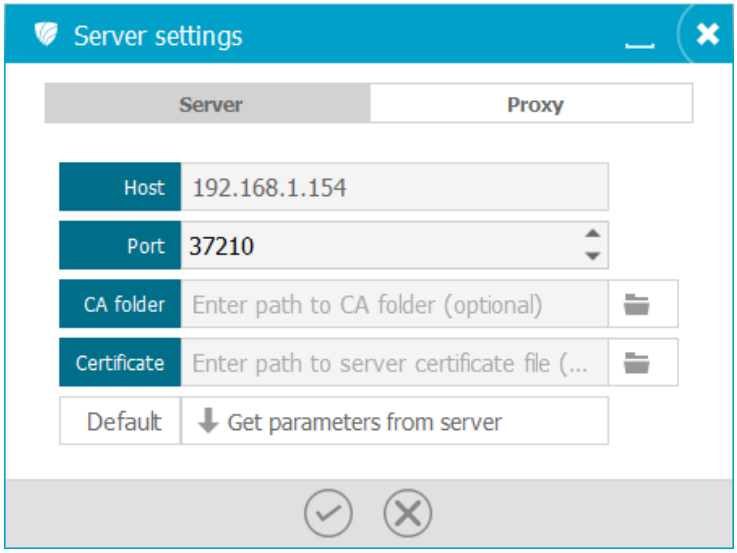
Using any starting method, you need to keep the starting order of the servers. First the Mongo server, then Redis, then vipole-server, then vipole-relay and the autoconfig server is the last one in the list (if you use it).

12. Starting the VIPole client application.

Click Skip to proceed. Enter VIPole ID and the admin password that you specified in sec.4.5.



Click on Settings and enter the domain name or the IP-address of your server in the «Host» field.

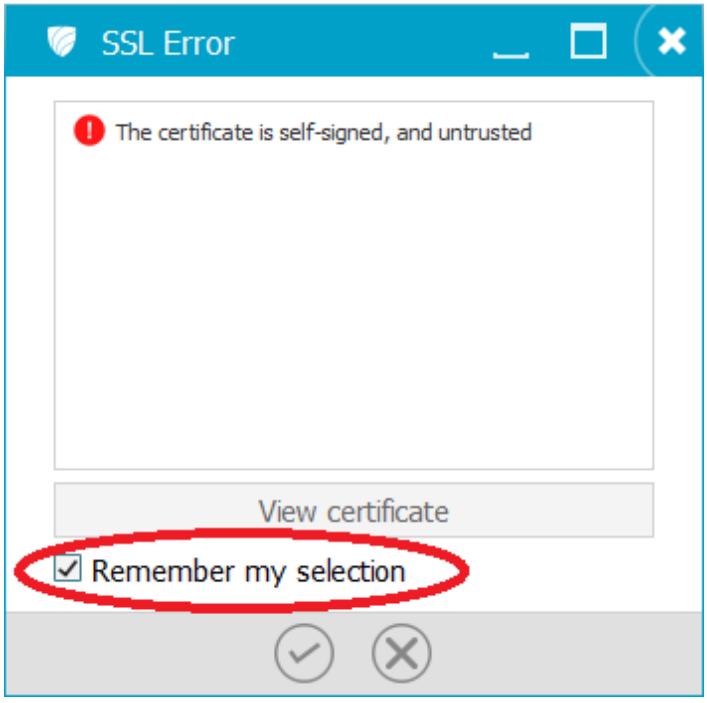


Note, that if you've entered the IP address instead of the domain name, you need to enter VIPole ID (Login) with the domain name, for example admin_login@example.com

Click on ✓.

Press the Log in button.

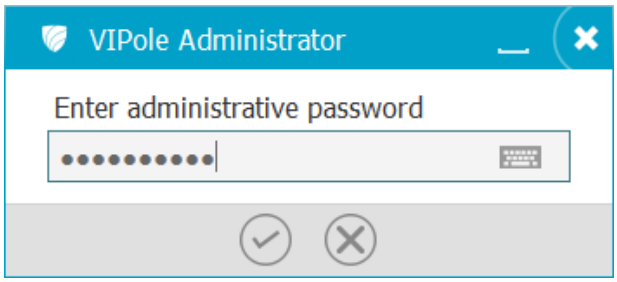
Since we are using the self-signed certificate now and we haven't specified the path to its local copy, we will receive the following message when connecting:



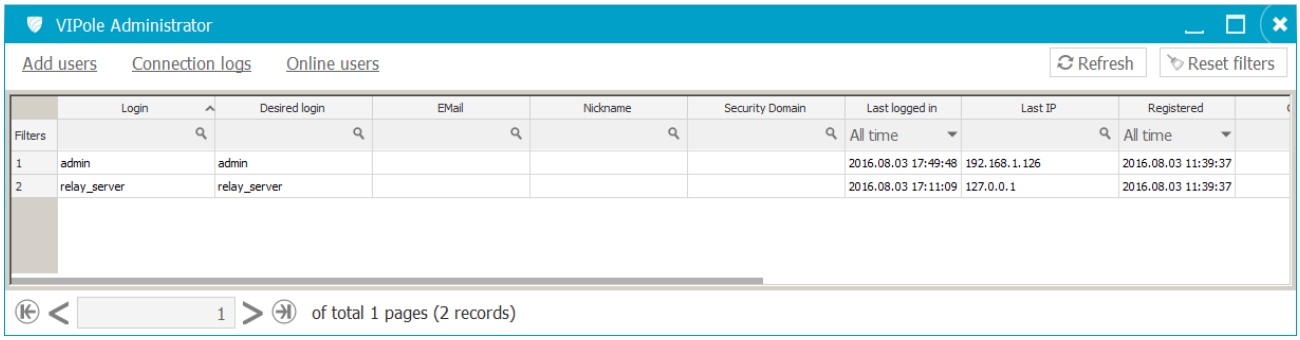
Check the «Remember my choice» box and click on ✓.

12.1. Generate the encryption keys and set the secret phrase (as you did during VIPole client application first run).

12.2. After you've launched the client application, go to Main menu -> Extensions ->VIPole administrator.



At the first launch of «VIPole administrator» panel, create the admin password and then enter it to manage the users of VIPole server.



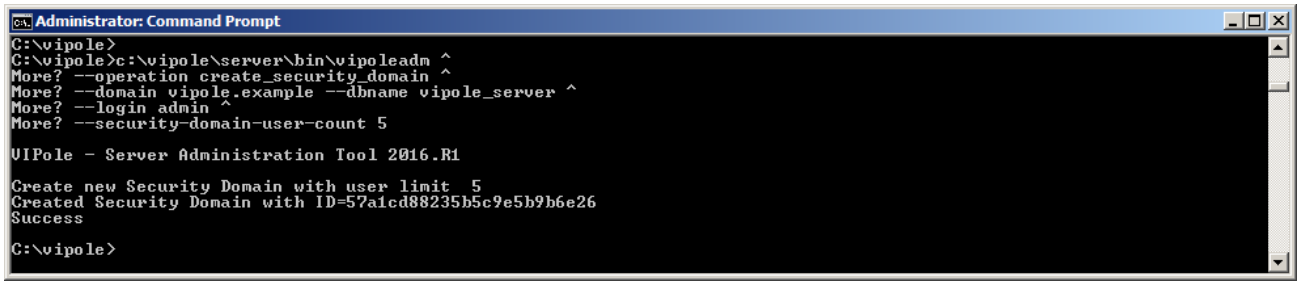
Note, that you haven't created a security domain yet and you manage all users of the server. Your powers include adding users, viewing the connection log and monitoring active sessions. See the list of additional user managing features in the Security domain account admin manual.

13. Advanced user management features

Setting secret phrases, configuring security settings and managing user contact lists are the features available only within a security domain (team account), which you need to create additionally.

You can create a security domain using the console utility **vipoleadm**

```
c:\vipole\server\bin\vipoleadm ^
--operation create_ security-domain ^
--domain vipole.example --dbname vipole_server ^
--login <admin login> ^
--security-domain-user-count <number of users>
```



The user that will be set as a security domain administrator will need to log out and then log in and enter the VIPole administrator pane Main menu -> Extensions -> VIPole administrator.

The **--login** <**admin login**> specifies the login of the user who will be considered the security domain owner. This may be either the server admin, or any newly added user. This user will be the security domain admin. When entering the «VIPole administrator» extension in the client application, he or she will get access to advanced user management features within the security domain.

The **--security-domain-user-count <number of users>** - parameter sets the limit of users assigned to the security domain.

You can create several security domains, for example, for different departments of your company. After the security domain is created, you can increase the limit of security domain users at any time by command.

```
c:\vipole\server\bin\vipoleadm ^
--operation add_security_domain_user_limit ^
--domain vipole.example --dbname vipole_server ^
--security-domain-user-count <number of users> ^
--security-domain-id <id>
```

--domain - your domain name

<number of users> - the number of users you want to add to the security domain.

<id > - the ID of the security domain where you are adding users. The security domain ID can be found on the Parameters tab of the VIPole administrator extension.

The total number of users in the created security domain cannot exceed the number of your VIPole Corporate Server user licenses.

The administrator can also delete users from the security domain.

```
c:\vipole\server\bin\vipoleadm ^
--operation move_user_from_security_domains ^
--domain vipole.example --dbname vipole_server --login <login>
```

--domain - your domain name

<login> - the login of the users you are deleting from the security domain

If you exceed the limit of users on the server, you need either to purchase additional user licenses (adding licenses is described in sec. 4.7-4.10) or to block extra users by the following command:

```
c:\vipole\server\bin\vipoleadm ^
--operation block_user ^
--domain vipole.example --dbname vipole_server --login <login>
```

--domain - your domain name

<login > - the login of the user you are blocking

Only active users are considered as security domain members within the license.