

VIPole Corporate Server

User Guide for Security Domain Administrator

v.3.0, 2016



VIPole
www.vipole.com

SECURE AND ENCRYPTED MESSENGER
for secure communications and encrypted data storage

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

Content

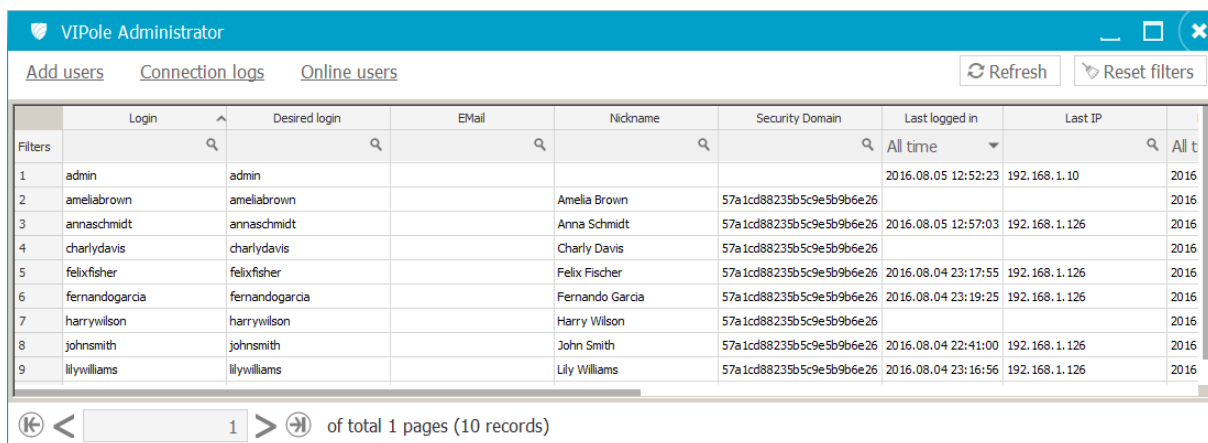
1. Introduction	3
2. Creation of a new Security domain.....	5
3. Getting started with the Security Domain.....	6
4. Administrator dashboard	7
4.1. First run of the administrator dashboard.....	7
4.2. Regular launch of the administrator dashboard.....	8
5. Application windows	9
5.1. User Administration window	10
5.1.1. Profile Tab	10
5.1.2. Connections Tab	11
5.1.3. Security Tab.....	12
5.1.4. Contact list Tab.....	16
5.1.5. Logs Tab	17
5.2. Parameters window	18
5.2.1. Parameters Tab	18
5.2.2. Administrators Tab	19
5.2.3. Security Templates Tab.....	20
5.2.4. Contactlist Templates Tab	21
5.2.5. Logs Tab	22
5.3. Add Users window	22
5.3.1. Single User Tab.....	23
5.3.2. Multiple Users Tab	24
5.3.3. Import Users Tab.....	25
5.3.4. LDAP tab.....	27
6. User Connection Logs window.....	34
7. Online Connection window.....	35

1. Introduction

Security domain enables you to manage a group of VIPole users. You can add new account users, delete users, block them and configure their security policy. You can assign passwords and secret phrases to users and assign contact lists for them.

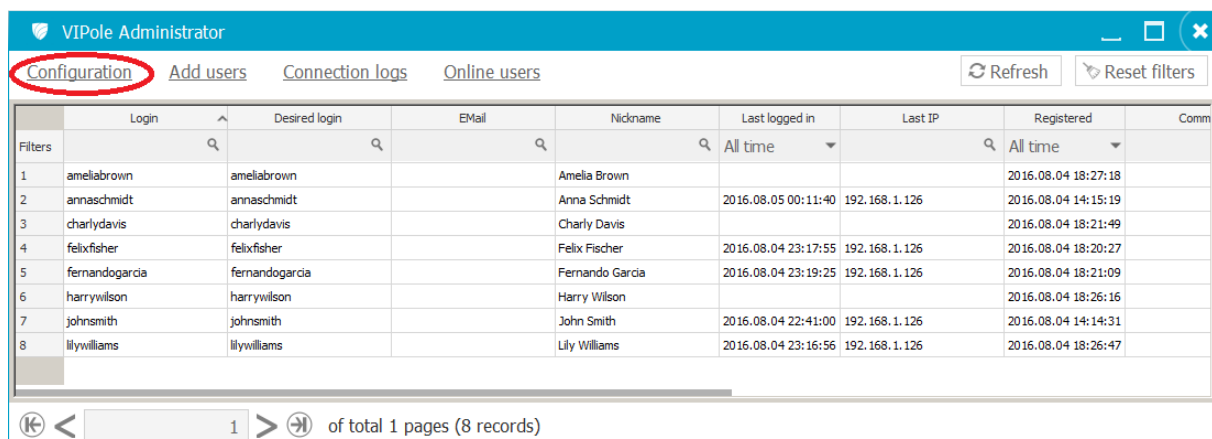
If you use a VIPole Corporate Server, we recommend you to create a Security domain for user management as it described in section 2 of this Guide and read the detailed VIPole Corporate Server Installation and Configuration Manual. The administrator of a Security domain has more opportunities for user management than the VIPole Corporate Server administrator (server administrator). Only part of the features is available to the server administrator.

Server administrator



	Login	Desired login	EMail	Nickname	Security Domain	Last logged in	Last IP
1	admin	admin				2016.08.05 12:52:23	192.168.1.10
2	ameliabrown	ameliabrown		Amelia Brown	57a1cd88235b5c9e5b9b6e26		
3	annaschmidt	annaschmidt		Anna Schmidt	57a1cd88235b5c9e5b9b6e26	2016.08.05 12:57:03	192.168.1.126
4	charlydavis	charlydavis		Charly Davis	57a1cd88235b5c9e5b9b6e26		
5	felixfisher	felixfisher		Felix Fischer	57a1cd88235b5c9e5b9b6e26	2016.08.04 23:17:55	192.168.1.126
6	fernandogarcia	fernandogarcia		Fernando Garcia	57a1cd88235b5c9e5b9b6e26	2016.08.04 23:19:25	192.168.1.126
7	harrywilson	harrywilson		Harry Wilson	57a1cd88235b5c9e5b9b6e26		
8	johnsmith	johnsmith		John Smith	57a1cd88235b5c9e5b9b6e26	2016.08.04 22:41:00	192.168.1.126
9	lilywilliams	lilywilliams		Lily Williams	57a1cd88235b5c9e5b9b6e26	2016.08.04 23:16:56	192.168.1.126

Security domain administrator



	Login	Desired login	EMail	Nickname	Last logged in	Last IP	Registered	Comm
1	ameliabrown	ameliabrown		Amelia Brown			2016.08.04 18:27:18	
2	annaschmidt	annaschmidt		Anna Schmidt	2016.08.05 00:11:40	192.168.1.126	2016.08.04 14:15:19	
3	charlydavis	charlydavis		Charly Davis			2016.08.04 18:21:49	
4	felixfisher	felixfisher		Felix Fischer	2016.08.04 23:17:55	192.168.1.126	2016.08.04 18:20:27	
5	fernandogarcia	fernandogarcia		Fernando Garcia	2016.08.04 23:19:25	192.168.1.126	2016.08.04 18:21:09	
6	harrywilson	harrywilson		Harry Wilson			2016.08.04 18:26:16	
7	johnsmith	johnsmith		John Smith	2016.08.04 22:41:00	192.168.1.126	2016.08.04 14:14:31	
8	lilywilliams	lilywilliams		Lily Williams	2016.08.04 23:16:56	192.168.1.126	2016.08.04 18:26:47	

Note! Unlike the Security domain administrator, the server administrator does not have access to passwords and encryption keys of the users.

Security domain administrator

ViPole user administration

Login: ameliabrown

Profile Connections **Security** Contactlist Logs

Apply security template

Security template: Default template [v] [Apply]

Export current settings as a security template

Security template: New [v] [Save]

Blocking

☐ Blocked

☐ Blocked in Security Domain

Permissions

☐ Online mode

☐ Limit contactlist to members of the Security Domain only

☒ Can change password

☒ Can change keys

☒ Can change fake secret phrase

☒ Can change program lock parameters

☒ Can change program auto logout parameters

☒ Can edit contactlist

☒ Can change messages burning mode

☒ Can change IP hiding for calls

☒ Can keep secret phrase locally for client autologin

☒ Can download files from server to client

Password

Password: [input]

Last changed: [input]

Secret phrase and keys

Secret phrase

Secret phrase: [input]

Keys records

ID	Created	Created by	Created from IP
[Empty table body]			

Auto logout

☐ Enable auto logout when idle

☐ Enable auto logout when offline

Program lock

Use to unlock: Secret phrase [v]

☐ Enable auto lock when idle

☐ Unmount encrypted ViPole storage when program is locked

Rapid unlock code

Rapid unlock code: [input]

Last changed: [input]

Fake secret phrase mode

Fake secret phrase mode: None [v]

Fake secret phrase

Fake secret phrase: [input]

Last changed: [input]

Contactlist

Who can send messages to me: Only authorized contacts [v]

Grant adding to contactlist: Always [v]

Messages burning

Mode: Adjustable per contact [v]

Hide IP during calls

Mode: Adjustable per contact [v]

Server administrator

ViPole user administration

Login: ameliabrown

Profile Connections **Security** Contactlist Logs

Blocking

☐ Blocked

☐ Blocked in Security Domain

Permissions

☐ Online mode

☐ Limit contactlist to members of the Security Domain only

☒ Can change password

☒ Can change keys

☒ Can change fake secret phrase

☒ Can change program lock parameters

☒ Can change program auto logout parameters

☒ Can edit contactlist

☒ Can change messages burning mode

☒ Can change IP hiding for calls

☒ Can keep secret phrase locally for client autologin

☒ Can download files from server to client

Password

Password: [input]

Last changed: [input]

Secret phrase and keys

Keys records

	Deleted	Deleted by	Deleted from IP
[Empty table body]			

Auto logout

☐ Enable auto logout when idle

☐ Enable auto logout when offline

Program lock

Use to unlock: Secret phrase [v]

☐ Enable auto lock when idle

☐ Unmount encrypted ViPole storage when program is locked

Fake secret phrase mode

Fake secret phrase mode: None [v]

Contactlist

Who can send messages to me: Only authorized contacts [v]

Grant adding to contactlist: Always [v]

Messages burning

Mode: Adjustable per contact [v]

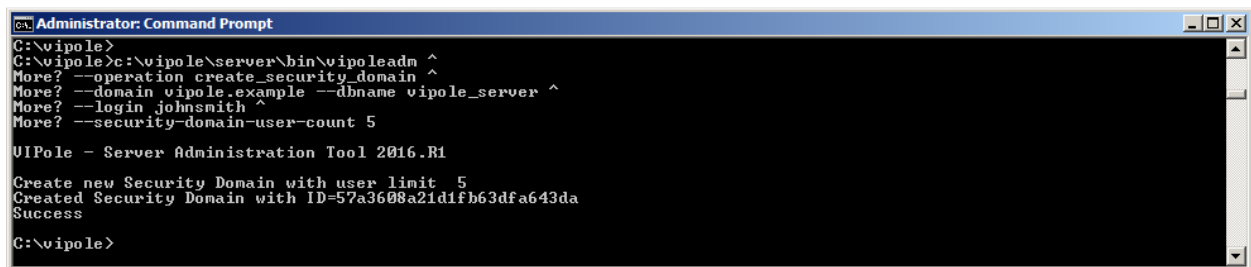
Hide IP during calls

Mode: Adjustable per contact [v]

2. Creation of a new Security domain

The server administrator can create a new Security domain by the following command

```
vipoleadm --domain vipole.example --operation create_security_domain --login  
<user login>  
--security_domain-user-count <number of users>
```



```
Administrator: Command Prompt
C:\vipole>
C:\vipole>c:\vipole\server\bin\vipoleadm ^
More? --operation create_security_domain ^
More? --domain vipole.example --dbname vipole_server ^
More? --login johnsmith ^
More? --security-domain-user-count 5
VIPole - Server Administration Tool 2016.R1
Create new Security Domain with user limit 5
Created Security Domain with ID=57a3608a21d1fb63dfa643da
Success
C:\vipole>
```

<user login> the login of the user that will be the owner of the Security domain. It can be a server administrator or any other newly added user. The selected user will be a Security domain administrator and will get advanced user management features for managing Security domain members.

<number of users> - user number limit in the Security domain.

You can create several Security domains for different groups of employees.

You can always extend the limit number of the created Security domain users.

```
vipoleadm --domain Vipole.example --operation add_security_domain_user_limit  
--security_domain-user-count <number of users> --security-domain-id <id>
```


--domain – your domain name.

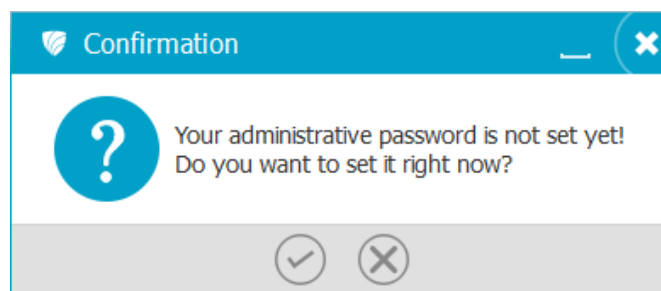
<number of users> - the number of users you want to add to Security domain.

<id> - The ID of the Security domain where you want to extend the user limit. You can find the Security domain ID in the Parameters window.

3. Getting started with the Security Domain

To manage the Security domain members, the built-in VIPole administrator panel is used that allows the Security Domain owner or the assigned administrator to manage users, their settings and activities:

1. Open the administrator panel. In the Main menu of VIPole for desktop, go to Extensions > VIPole Administrator.
2. Set the administrator password. Click on , then enter and repeat the password that you will enter every time for administering the Security Domain.

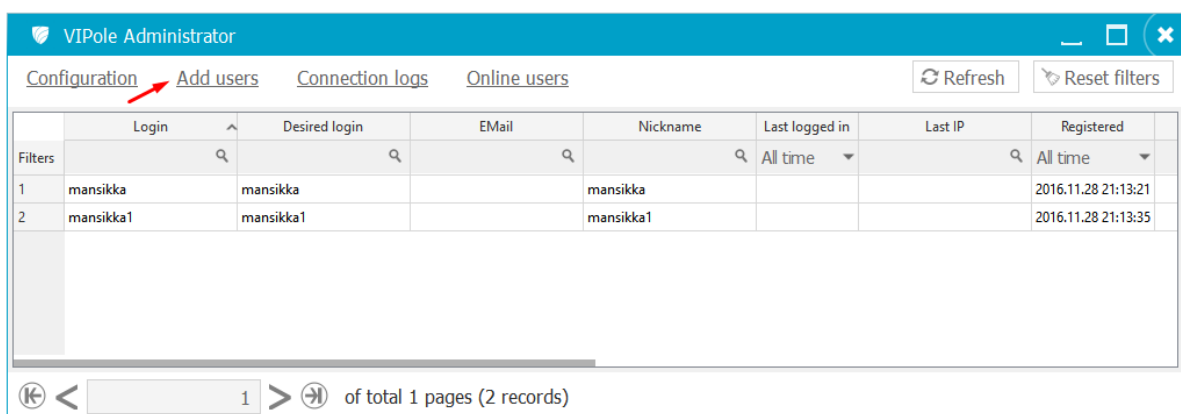


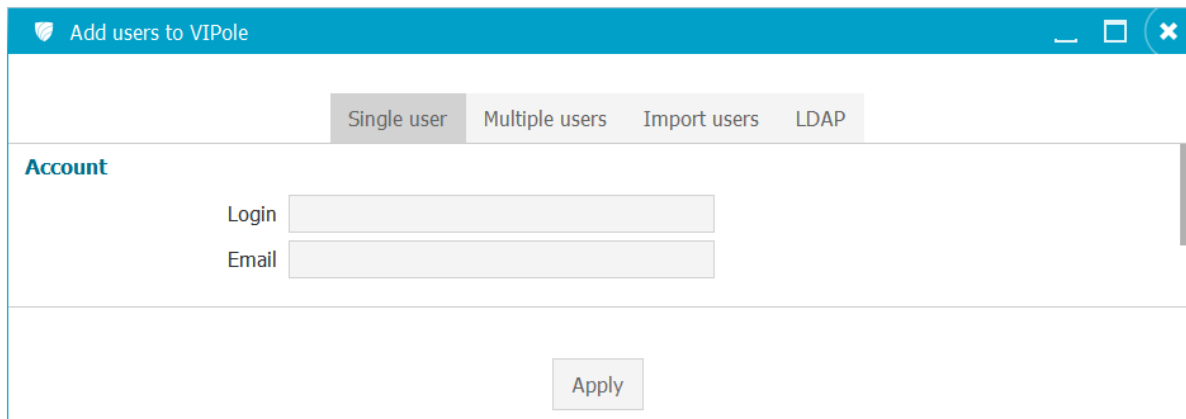
The admin panel displays information about the Security Domain members, and here you can create new user accounts.

Please note, that by default the owner of the Security Domain is not included into it, because he or she can own several accounts.

To create new users:

1. Go to the «Add users» tab:





2. Create a new user. Set a login, a password, choose the user package where you want to add this user, fill the necessary fields, and click on «Apply».

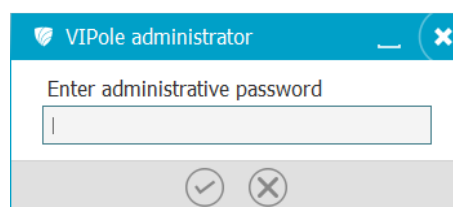
Depending on the desired level of control, the administrator can assign passwords and secret phrases to users or allow them to generate the encryption keys independently. When assigning the secret phrase, the administrator gets access to the conversations and files of the Security Domain user.

4. Administrator dashboard

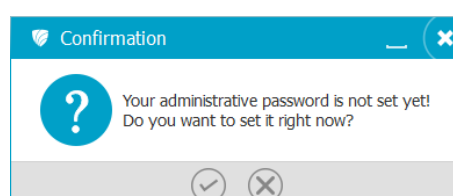
4.1. First run of the administrator dashboard

A built-in extension in the client application is used for user management of the Security domain. The extension is called via the Main menu option Extensions> VIPole Administrator.

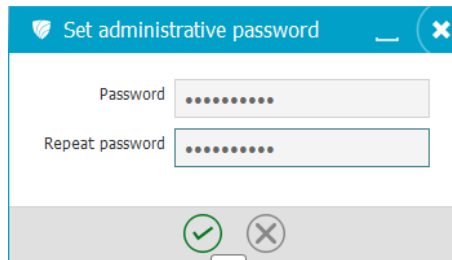
When you launch the extension to manage the Security domain, you need to enter the admin password.



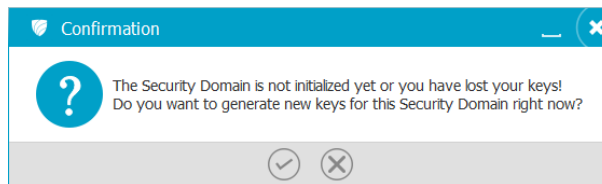
On the first run, you will need to set the password.



Set and confirm the administrative password for the Security domain.

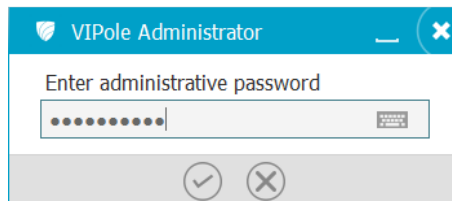
A dialog box titled "Set administrative password" with a shield icon. It contains two password input fields: "Password" and "Repeat password", both filled with dots. At the bottom, there are two circular buttons: a green checkmark and a grey 'X'.

Security domain encryption keys will be generated automatically.

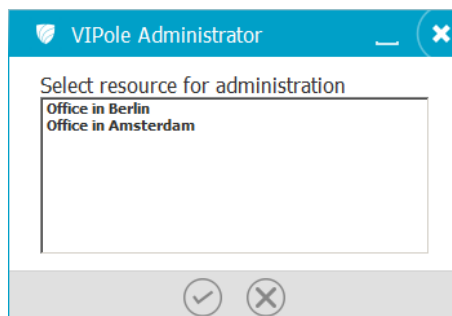
A dialog box titled "Confirmation" with a shield icon. It features a blue circle with a white question mark. The text inside reads: "The Security Domain is not initialized yet or you have lost your keys! Do you want to generate new keys for this Security Domain right now?". At the bottom, there are two circular buttons: a green checkmark and a grey 'X'.

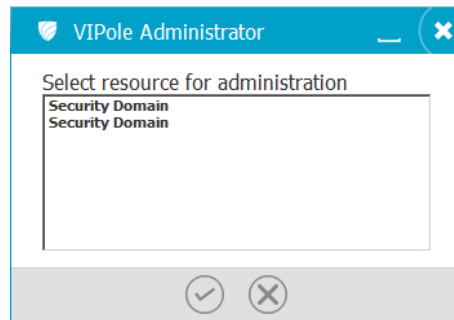
4.2. Regular launch of the administrator dashboard

Every time you run the extension to manage the Security domain you need to enter your admin password.

A dialog box titled "VIPole Administrator" with a shield icon. It contains a single password input field labeled "Enter administrative password" with dots. At the bottom, there are two circular buttons: a green checkmark and a grey 'X'.

If you have more than one Security domain, you need to choose the ID of the account you want to administer.

A dialog box titled "VIPole Administrator" with a shield icon. It contains a list box labeled "Select resource for administration" with two items: "Office in Berlin" and "Office in Amsterdam". At the bottom, there are two circular buttons: a green checkmark and a grey 'X'.



Then the Security domain management window will open with a list of the members of the domain.

VIPole Administrator								
Configuration Add users Connection logs Online users					Refresh		Reset filters	
	Login	Desired login	EMail	Nickname	Last logged in	Last IP	Registered	Comm
Filters					All time		All time	
1	ameliabrown	ameliabrown		Amelia Brown			2016.08.04 18:27:18	
2	annaschmidt	annaschmidt		Anna Schmidt	2016.08.04 22:30:53	192.168.1.206	2016.08.04 14:15:19	
3	charlydavis	charlydavis		Charly Davis			2016.08.04 18:21:49	
4	felixfisher	felixfisher		Felix Fischer	2016.08.04 23:17:55	192.168.1.109	2016.08.04 18:20:27	
5	fernandogarcia	fernandogarcia		Fernando Garcia	2016.08.04 23:19:25	192.168.1.126	2016.08.04 18:21:09	
6	harrywilson	harrywilson		Harry Wilson			2016.08.04 18:26:16	
7	johnsmith	johnsmith		John Smith	2016.08.04 22:41:00	192.168.1.104	2016.08.04 14:14:31	
8	lilywilliams	lilywilliams		Lily Williams	2016.08.04 23:16:56	192.168.1.14	2016.08.04 18:26:47	

5. Application windows

The Security domain management system includes four tabs:

- Configuration
- Add users
- Connection logs
- Online users

Below you will find the detailed description of each tab.

By right clicking on a user login, the menu appears:

	Login	Desired login	EMail	Nickname	Last logged in	Last IP	Registered	Comm
1	amelabrown			Amelia Brown			2016.08.04 18:27:18	
2	annaschmidt			Anna Schmidt	2016.08.05 12:57:03	192.168.1.206	2016.08.04 14:15:19	
3	charlydavis			Charly Davis			2016.08.04 18:21:49	
4	felixfisher			Felix Fischer	2016.08.04 23:17:55	192.168.1.109	2016.08.04 18:20:27	
5	fernandogarcia			Fernando Garcia	2016.08.04 23:19:25	192.168.1.126	2016.08.04 18:21:09	
6	harrywilson			Harry Wilson			2016.08.04 18:26:16	
7	johnsmith			John Smith	2016.08.04 22:41:00	192.168.1.104	2016.08.04 14:14:31	
8	lilywilliams			Lily Williams	2016.08.04 23:16:56	192.168.1.14	2016.08.04 18:26:47	

- **View/Edit user** opens the User Administration window. This window also opens by double-clicking.
- **Expel** deletes a user from the Security domain. After deleting a user from a Security domain, the administrator of the account can't configure this user settings anymore.
- **Delete user** deletes the user profile. All user data are no longer available.
- **Copy text** copies selected text in the table to the clipboard.

5.1. User Administration window

5.1.1. Profile Tab

On the Profile tab, you can edit the personal settings of the users that are available in the My profile menu of the client application.

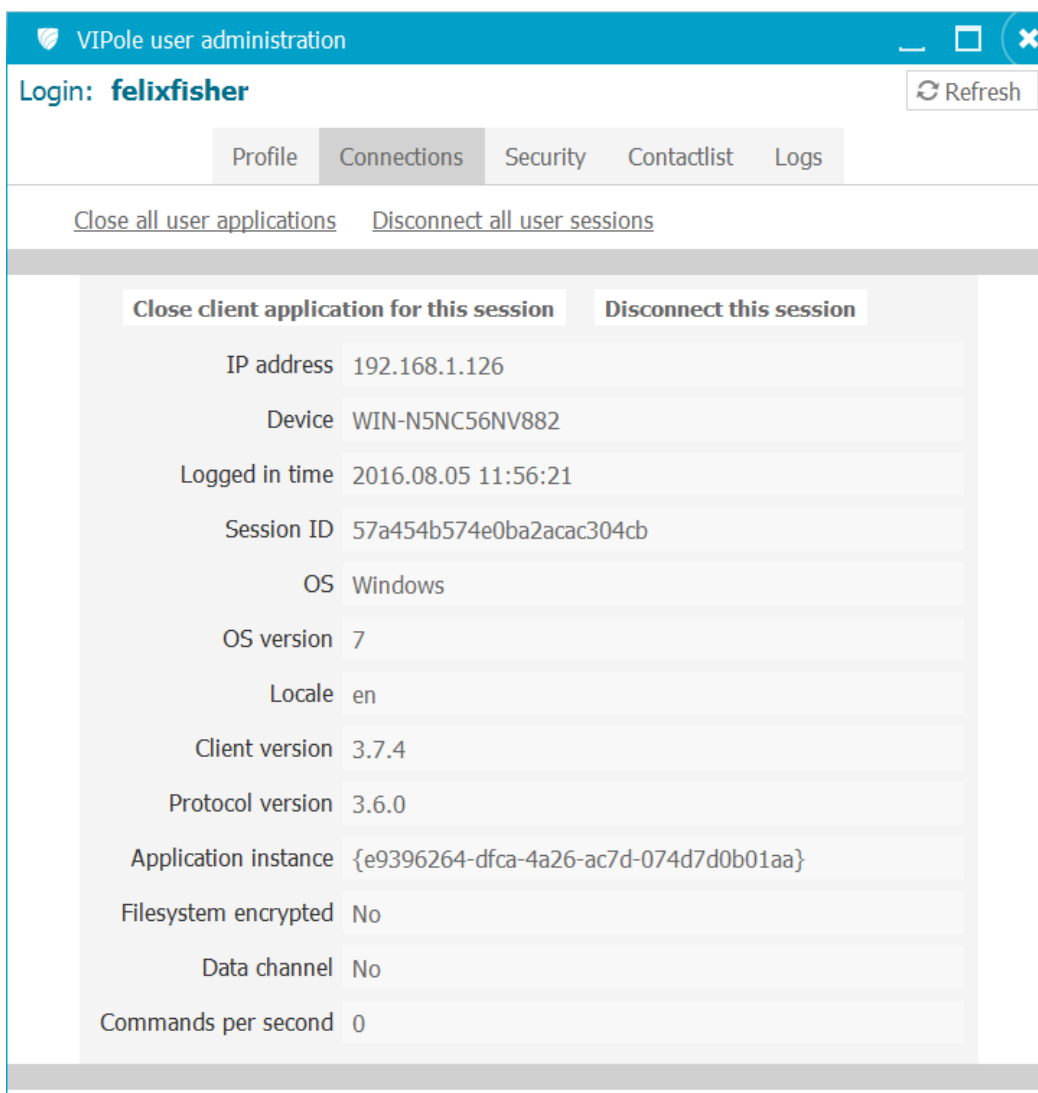
There are two additional sections available for Security domain administrator:

- **Extra details for administrator** – is used for storing user data identifying the user of the Security domain.
- **SIP parameters for VoIP** – this section is available for VIPole Corporate Server with enabled SIP module. User SIP ID and password are set on this tab, other connection settings are made by server administrator during server configuration.

The screenshot shows the 'VIPole user administration' window. At the top, the login is 'felixfisher' with a 'Refresh' button. Below this are tabs for 'Profile', 'Connections', 'Security', 'Contactlist', and 'Logs'. The 'Profile' tab is active, showing an 'Emergency' section with 'Clear messages history' and 'Block user' buttons. The 'General information' section displays the 'VIPole ID' as 'felixfisher' and the 'Nickname' as 'Felix Fischer'. The 'Extra details for administrator' section includes fields for 'Desired login' (felixfisher), 'EMail', 'Security Domain' (57a1cd88235b5c9e5b9b6e26), 'Comments', and 'Tags'. At the bottom, there is an 'Image' section with a placeholder icon for a user profile picture.

5.1.2.Connections Tab

On this tab, the administrator of the Security domain can quickly close a client program or disconnect it from the server. In case of multiple connections, it is possible to disable them individually or all at once.



5.1.3. Security Tab

Some settings on the Security tab correspond to the security settings of the client program. These settings can be used for the initial configuration of the security settings for the new user of the Security domain.

Later the user can change the security settings at his discretion. The Security domain administrator can prevent users from changing these settings – all of them or selectively.

Please note, that the Security tab which is available for the server administrator does not allow to change keys and secret phrases.

VIPole user administration

Login: felixfisher

Refresh

ProfileConnectionsSecurityContactlistLogs

Apply security template

Security template: Default template

Apply

Export current settings as a security template

Security template: New

Save

Blocking

☐ Blocked

☐ Blocked in Security Domain

Permissions

☐ Online mode

☐ Limit contactlist to members of the Security Domain only

☒ Can change password

☒ Can change keys

☒ Can change fake secret phrase

☒ Can change program lock parameters

☒ Can change program auto logout parameters

☒ Can edit contactlist

☒ Can change messages burning mode

☒ Can change IP hiding for calls

☒ Can keep secret phrase locally for client autologin

☒ Can download files from server to client

Password

Password

Last changed

Secret phrase and keys

Secret phrase

Secret phrase

Keys records

ID	Created	Created by	Created from IP		Deleted
----	---------	------------	-----------------	--	---------

Auto logout

☐ Enable auto logout when idle

☐ Enable auto logout when offline

Program lock

Use to unlock: Secret phrase

☐ Enable auto lock when idle

☐ Unmount encrypted VIPole storage when program is locked

Rapid unlock code

Rapid unlock code

Last changed

Fake secret phrase mode

Fake secret phrase mode: None

Fake secret phrase

Fake secret phrase

Last changed

Blocking

- **Blocked:** the user is blocked on the server. This option is available only for the server administrator.
- **Blocked in the Security domain:** the Security domain administrator can block any user and deny him access to the server.

Permissions

- **Online mode:** the user is allowed to use the client program only when he is connected to the server. In this mode, it is impossible to use the client program offline, for example, to view messages and notes.

This mode makes it possible to deny the user access to the data that is stored on the user's device. To accomplish this, block the user on the Security tab and close the user's client program on the Connections tab of the User administration window. After that, you can be sure that no one has access to the data stored on the user's device.

- Other permissions allow users to change the corresponding security settings in their profiles.

The remaining sections correspond to the Security page of the client program. These settings are forced in the client program, to which this template is assigned.

Password

- The Security domain administrator can set or change any user's password. This is the password to access the server. It shouldn't be confused with the secret phrase.

Secret phrase and keys

- The Security domain administrator can generate encryption keys and set secret phrases for users.

Auto logout

- In this section, you can set the time after which the user's profile will be closed automatically.
- You can set separately the user's idle time and offline time for automatic logout.

Program lock

- In this section, you can set the code for unlocking the program: a password to the server, a secret phrase or a special fast unlock code.
- You can also set the user idle time to lock the program. When the program is locked, all the open windows are collapsed.

Fast unlock code

- In this section, you can set the code used to unlock the program if a fast unlock code was chosen as an option for unlocking the program.

Fake secret phrase mode

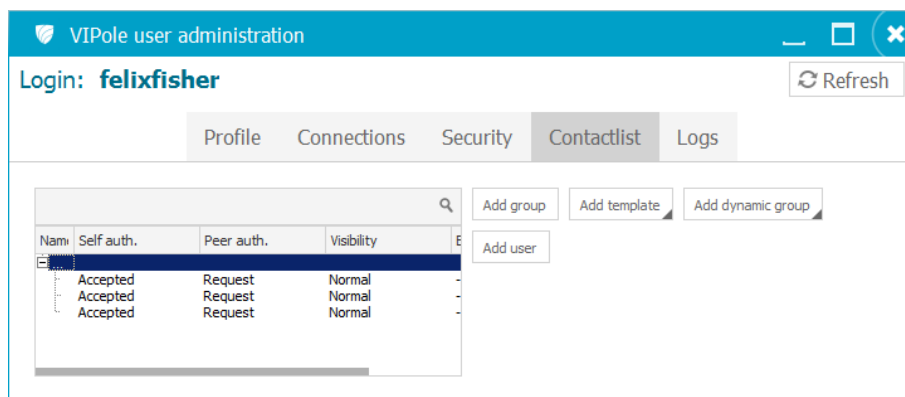
- This mode is used to protect the user data, if the user is forced to enter a secret phrase to access the data. The mode makes it possible to set a fake secret phrase and select a response of the client program to entering such a phrase:
 - *no*: the mode is not used
 - *program crash*: program crash occurs
 - *delete profile and then crash*: before the program crash, the local copy of the data is deleted.

Fake secret phrase

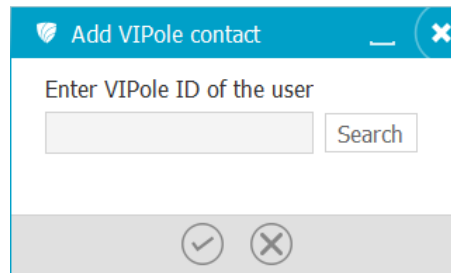
- Enter the fake secret phrase to activate data protection if the user is forced to open the profile.

5.1.4. Contact list Tab

Contact list tab makes it possible to fill in the user's contact list without having to request authorization and receiving permission for authorization. Adding to the contact list is mutual: the user will also be added to the contact list of the users who are in his contact list.



- **Add Group:** adds the name of the group to the contactlist. A group is used to structure contacts basing on some characteristic.
- **Add user:** add a contact to the group. Click on the group name, then click "Add user". Adding is done in the same way as in the client program. Enter the VIPole ID of the user you want to add, make sure that the contact exists in the system using search, and then add him by clicking ☑ Mutual authentication is done automatically.

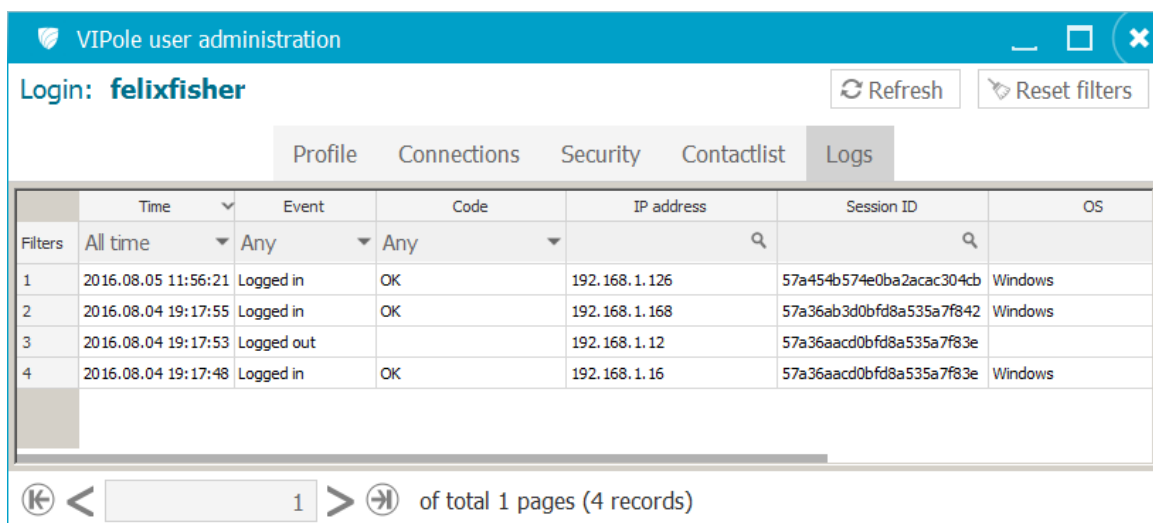


A dialog box titled "Add ViPole contact" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Enter ViPole ID of the user" and a "Search" button to its right. At the bottom of the dialog, there are two circular buttons: one with a checkmark and one with an 'X'.

- **Add template:** add contacts which are united into groups and currently listed in the specified template. The template is useful if you need to create the same contact lists for multiple users. A user for whom a contact list template is added, will also be included into the contact lists of all users listed in the template. Contacts that are subsequently added to the template, are not automatically copied to the contact list of the current user.
- **Add dynamic group:** the user is included into a dynamic group with the specified name. In this case, the contacts included into this dynamic group will be added to this user's contact list. Subsequently new members of the dynamic group will be added to the contact list of this user.

5.1.5. Logs Tab

Here you can track events that are related to the user.



The screenshot shows the "ViPole user administration" window. The "Login" field displays "felixfisher". There are "Refresh" and "Reset filters" buttons. Below the login field are tabs for "Profile", "Connections", "Security", "Contactlist", and "Logs", with "Logs" being the active tab. The main area contains a table with the following data:

	Time	Event	Code	IP address	Session ID	OS
Filters	All time	Any	Any			
1	2016.08.05 11:56:21	Logged in	OK	192.168.1.126	57a454b574e0ba2acac304cb	Windows
2	2016.08.04 19:17:55	Logged in	OK	192.168.1.168	57a36ab3d0bfd8a535a7f842	Windows
3	2016.08.04 19:17:53	Logged out		192.168.1.12	57a36aacd0bfd8a535a7f83e	
4	2016.08.04 19:17:48	Logged in	OK	192.168.1.16	57a36aacd0bfd8a535a7f83e	Windows

At the bottom of the window, there is a pagination bar showing "1" of total 1 pages (4 records).

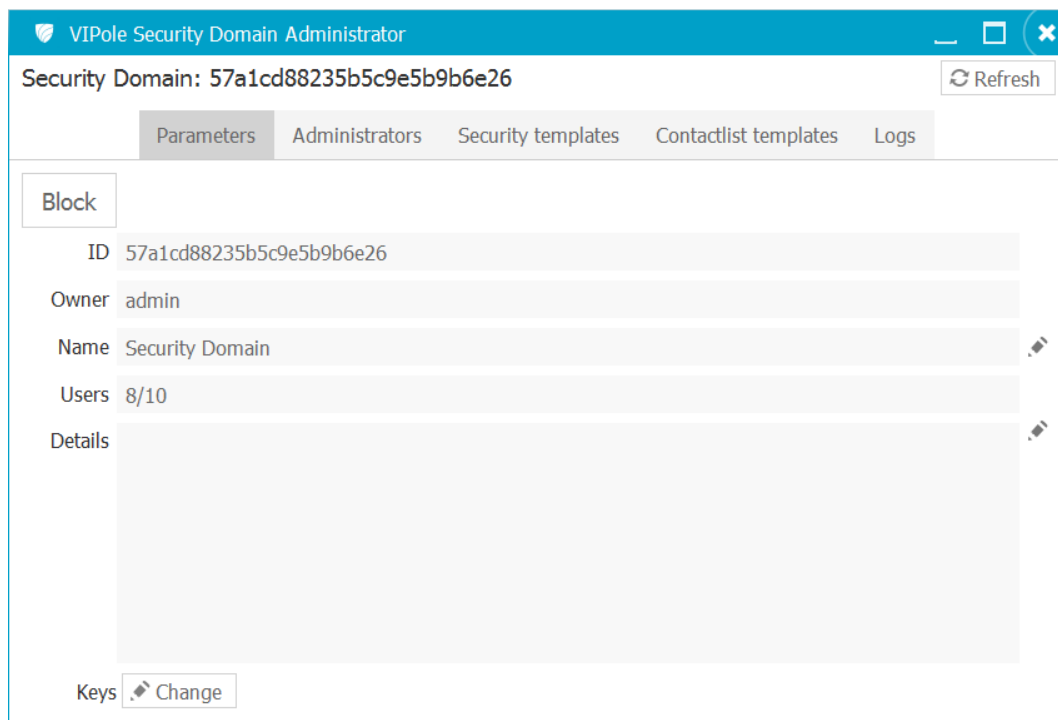
5.2. Parameters window

The Parameters window contains the following tabs:

- **Parameters** - basic account settings, including list of user packages.
- **Administrators** - list of administrators of the Security domain. Adding and deleting administrators.
- **Security templates** - centralized configuration of client programs of the members of the Security domain.
- **Contactlist templates** - providing a ready contact list for the members of the Security domain.
- **Logs** - viewing administrator activity logs.

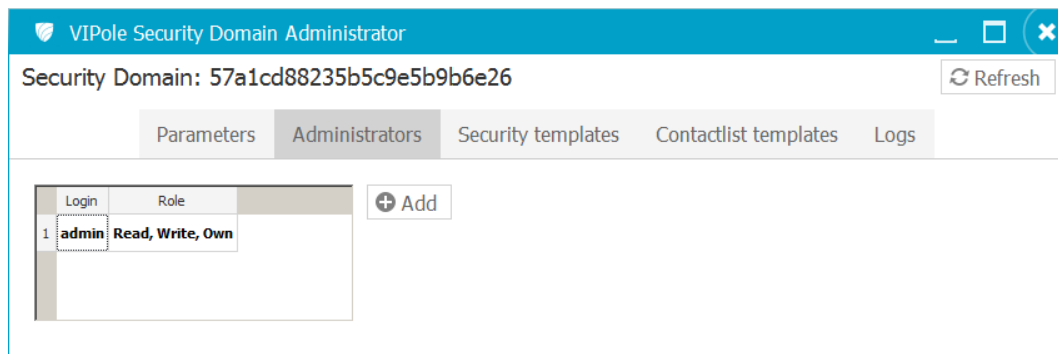
5.2.1. Parameters Tab

On this tab, you can find the current number of the users assigned to the Security domain.



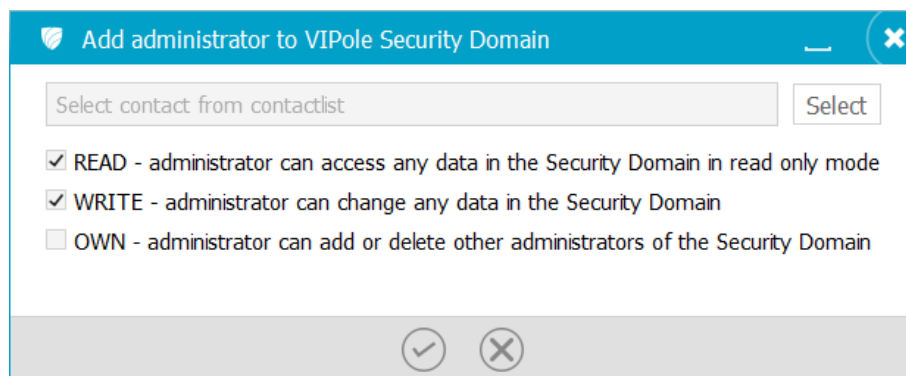
5.2.2. Administrators Tab

On this tab, you can add an administrator for the Security domain.



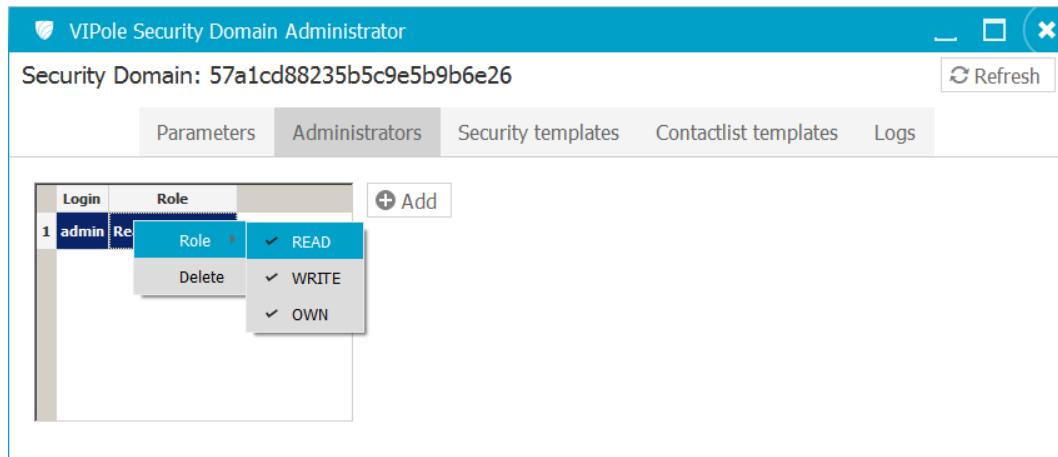
To add a new administrator:

- Click the Add button.
- By clicking Select, you can select a new administrator from the list of the members of the Security domain.



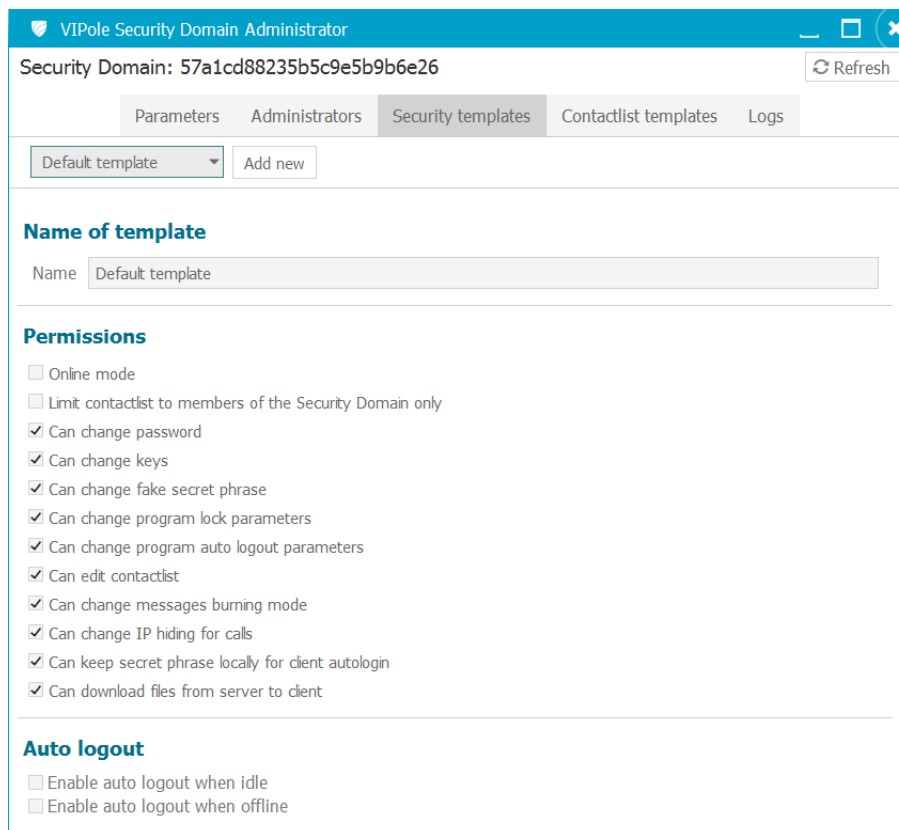
- Choose the rights of the new administrator and click ✓

By right clicking on the name of the administrator, you can edit his rights or delete him completely.



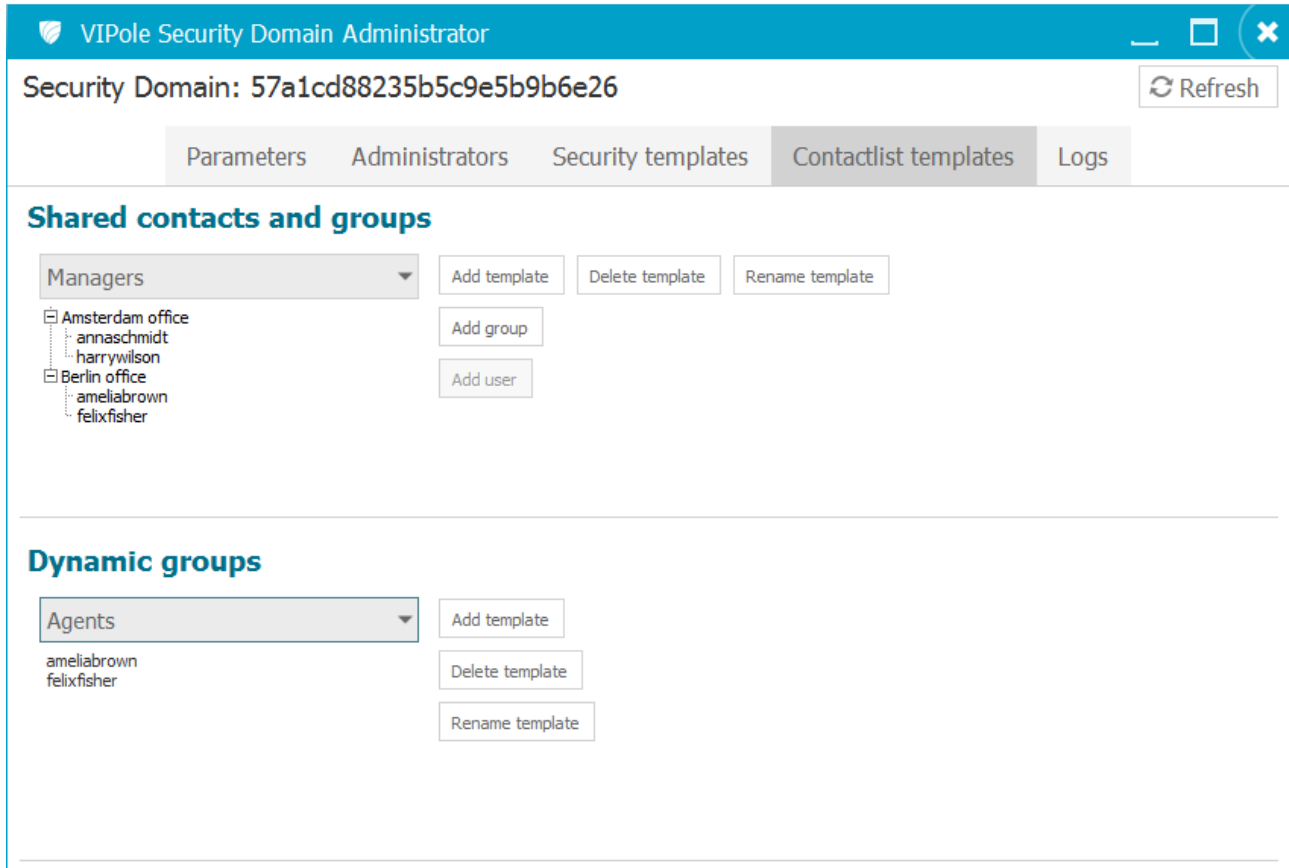
5.2.3. Security Templates Tab

Specify the name of the security template for fast search and further use. Description of the sections of the security template can be found in the description of the Security tab of the User administration window.

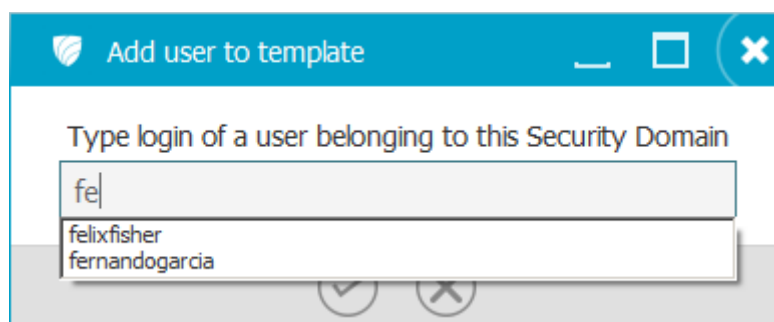


5.2.4. Contactlist Templates Tab

Here the Security domain administrator creates and edits templates of the users' contact lists. On this tab, you can also add, remove, or rename dynamic contact groups.



To add a user to a contact list template, you should first select a group.



Start typing the VIPole ID. After you type the second character, a prompt will appear with logins of the users of the Security domain.

5.2.5. Logs Tab

On this tab, you can view activity logs of the Security domain administrators.

VIPole Security Domain Administrator

5.3. Add Users window

In this window, you can manage the members of the Security domain. You can add individual users and groups of users, or import user data from a CSV file.

When you add a single user, you can fill in his profile and generate encryption keys.

After adding a user, you need tell him the password and the secret phrase. You can also add users by importing data from a file.

When you add a group, logins are generated automatically by adding numbers in the end of the letter prefix.

5.3.1. Single User Tab

To add a single user:

- Specify the login, password, and confirm password.
- After that, select the user package and click Apply.

A user package is used to count the number of users in the Security domain.

The screenshot shows a web application window titled "Add users to VIPole". It has three tabs: "Single user" (selected), "Multiple users", and "Import users". The "Single user" tab contains three main sections: "Account", "Keys", and "Templates".

Account section:

- Fields for "Login", "Email", "Password", and "Repeat password". The "Password" field has icons for visibility, copy, and settings.
- Fields for "Nickname", "First name", "Middle name", and "Last name".
- Two checkboxes: "Set fake secret phrase" and "Set application unlock code".

Keys section:

- A checkbox labeled "Generate keys".

Templates section:

- "Security template" dropdown menu with "Default template" selected.
- "Shared contactlist template" dropdown menu with "None" selected.
- "Dynamic contactlist group" dropdown menu with "None" selected.
- "Tags" dropdown menu with "None" selected and an "Add new" link below it.
- A "Comments" text area.

At the bottom right of the window is an "Apply" button.

5.3.2. Multiple Users Tab

To add multiple users:

- Specify the initial characters of the logins and the number of added users.
- After that, select the user package and click Apply.

A user package is used to count the number of users in the Security domain.

User logins will be created by adding a number to the initial set of characters.

The screenshot shows a window titled "Add users to VIPole" with a blue header bar. Inside, there are three tabs: "Single user", "Multiple users" (which is selected and highlighted), and "Import users". The "Multiple users" tab contains three sections: "Account", "Keys", and "Templates".

Account

- "Login starts with" is a text input field.
- "Count" is a numeric spinner set to "1".
- There are two checkboxes: ☐ "Generate fake secret phrases" and ☐ "Generate application unlock codes".

Keys

- There is one checkbox: ☐ "Generate keys".

Templates

- "Security template" is a dropdown menu showing "Default template".
- "Shared contactlist template" is a dropdown menu showing "None".
- "Dynamic contactlist group" is a dropdown menu showing "None".
- "Tags" is a dropdown menu showing "None" and "Add new".
- "Comments" is a large text area.

At the bottom center of the dialog is an "Apply" button.

5.3.3. Import Users Tab

On this tab, you can add a group of users from a text file or Excel .CSV file.

Add users to VIPole
— □ ×

Single user
Multiple users
Import users

Account

CSV file ; CSV separator ☒ CSV with header

☐ In case of login conflicts append numbers to logins that already exist on the server

	Status	Registered login	Desired login ^	EEmail	Nickname	First name	Middle name	Last name	Comments	Passw
1			EmilyDavies5	EmilyDavies5@example.com	EmilyDavies5	Emily	Davies		Comment3	From tal
2			OliviaWilson5	OliviaWilson5@example.com	OliviaWilson5	Olivia	Wilson		Comment	From tal
3			ThomasMiller5	ThomasMiller5@example.com	ThomasMiller5	Thomas	Miller		Comment2	From tal

Keys

☐ Generate keys

Templates

Security template

Default template ▼

Shared contactlist template

None ▼

Dynamic contactlist group

None ▼

Tags

None
Add new

To import a group of users from a file:

- Create an Excel spreadsheet with the following fields (the fields can have any name, the order is important).

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	DESIRED_LOGIN	EMAIL	NICKNAME	NAME1	NAME2	NAME3	COMMENTS	PASSWORD_MODE	SECRET_PHRASE_MODE	UNLOCK_CODE_MODE	FAKE_SECRET_MODE	PASSWORD	SECRET_PHRASE	UNLOCK_CODE	FAKE_SECRET	
1																
2	ThomasMiller	ThomasMiller@example.com	ThomasMiller	Thomas	Miller		Comment2	1	0	1	2	password2	secret-phrase2	unlock-code2	fake-secret2	
3	OliviaWilson	OliviaWilson@example.com	OliviaWilson	Olivia	Wilson		Comment	1	1	1	1	password	secret-phrase	unlock-code	fake-secret	
4	EmilyDavies	EmilyDavies@example.com	EmilyDavies	Emily	Davies		Comment3	1	2	2	2	password3	secret-phrase3	unlock-code3	fake-secret3	
5																
6																
7																
8																

DESIRED_LOGIN – the original login. If this login already exists, it is possible to automatically add digits to get a new login.

EMAIL – the user' s email address

NICKNAME – the user' s nickname

NAME1 – the user' s first name

NAME2 – the user' s patronymic

NAME3 – the user' s surname

COMMENTS – comments to the account

PASSWORD_MODE –

- 1 – the password is taken from an uploaded table
- 2 – the password is generated automatically

SECRET_PHRASE_MODE –

- 0 – ignored (the user has to generate a secret phrase by himself)
- 1 – the password is taken from an uploaded table
- 2 – the password is generated automatically

UNLOCK_CODE_MODE –

- 0 – ignored (the user has to generate the unlock code by himself)
- 1 – the unlock code is taken from an uploaded table
- 2 – the unlock code is generated automatically

FAKE_SECRET_MODE –

- 0 – ignored (the user has to generate a fake secret phrase by himself)
- 1 – the fake secret phrase is taken from an uploaded table
- 2 – the fake secret phrase is generated automatically

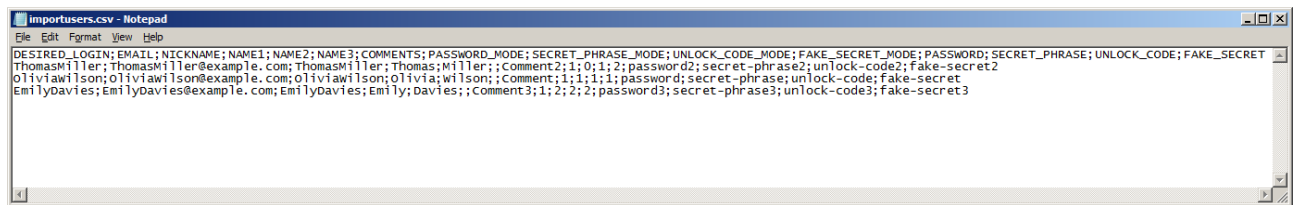
PASSWORD – the password to log into the personal account on the site and to download profile

SECRET_PHRASE – the secret phrase

UNLOCK_CODE – unlock code

FAKE_SECRET – fake secret phrase

- Save the table as CSV. This is a text file of the following format:



- In the CSV separator field place the symbol “;” or the one you used for separating the fields.
- A check mark in the field “CSV with header” means that the first row of the CSV file contains the field names, as in the example.
- Click the Browse button and select a file to import. Imported user entries will appear in the table. If an error occurs during import, for example, if you have specified an invalid e-mail, in the Status column a red message will appear to explain the error.
- After that, select the user package to which you want to add users. Specify templates which will be applied to all imported users and click the Apply button.

5.3.4 LDAP tab

Integration with LDAP (Lightweight Directory Access Protocol) significantly accelerates the deployment of VIPole Corporate server, since there is no need to manually enter the data of new users into the system.

There are two ways to integrate Microsoft Active Directory(AD)/LDAP with VIPole server:

1. Import users to VIPole database from AD/LDAP.
 - In this case, user passwords are not imported.
 - User authentication when they are connecting to VIPole server is performed via the AD/LDAP server.
2. Exporting users from AD/LDAP to a CSV file.
 - CSV file can be imported to the VIPole server database (possible, if necessary, after editing).
 - In this case, passwords are generated automatically or taken from the CSV file.

Importing users to VIPole Security Domain is performed by the Domain owner.

To get started with AD/LDAP server, configure the VIPole server using the following configuration file settings **server.config**:

Turn on the AD/LDAP support

ldap-enabled = 1

Specify the unique name (DN) of the AD/LDAP user, who is allowed to import data from the AD / LDAP tree

ldap-admin-dn = CN=Admin,CN=Users,DC=vipole,DC=ldap,DC=sample

Specify the password of the user who is allowed to import data

ldap-admin-password = SecretPassword

URI of the AD/LDAP server

ldap-uri = ldap://192.168.1.155

The DN, from which the search of users in the subtree is started (there must be at least one user in the subtree so that VIPole server could check the correctness of connection to the AD / LDAP server)

ldap-users-search-base = CN=Users,DC=vipole,DC=ldap,DC=sample

The name of the attribute that is used as a user's login

ldap-users-login-mapping=cn

After you configure these settings, restart VIPole server.

Importing users from AD/LDAP to VIPole database.

Importing users is performed using the vipole-ldap console utility or using the «VIPole Administrator» extension of the client program.

Importing users using the vipole-ldap console utility:

The parameters of vipole-ldap utility are set on the command line:

-l [--login] – the login of the administrator of VIPole security Domain, where users will be imported.

--passwd – the administrator password specified by the **--login** parameter.

--passwd-file – the file with the administrator password (used instead of **--passwd**).

--domain – the domain name of your VIPole server (the name that is added to a login after the @ symbol, e.g. admin@example.com)

--server-host arg (=127.0.0.1)– the IP address of VIPole server

--server-port arg (=37210)– the port of VIPole server.

--certificate arg - the path to file of the VIPole server chain of certificates that is specified in the parameter **certificate-chain-file** in the server.config file.

--security-domain arg - the identifier of the Security Domain (must be specified if the domain administrator has several domains). The identifier is shown when the Security Domain is created, and also it is displayed on the «Parameters» tab of the «VIPole Administrator» extension of the client application.

--admin-password arg – the administrator password for managing the Security Domain (this password is created when you first run the «VIPole Administrator» extension).

--base-dn arg – the DN, from which the search of users is started. If not specified – used as the **ldap-users-search-base** parameter of the configuration file of VIPole server.

--filter arg

(=(&(&(objectCategory=person)(objectClass=user))(objectClass=inetOrgPerson)) – the filter of user accounts according to which the selection is performed. For detailed syntax and examples, see [Active Directory: LDAP Syntax Filters](#).

--skip-imported [0|1] (=0)– skipping the existing users during the import.

--morph-login - in the case of user login duplication adds a unique number to the end of the login.

-t [--timeout] arg (=300)- wait time for the AD/LDAP server response in seconds.

--dry-run – users are not added to the database, and the information about the users who have been added is displayed.

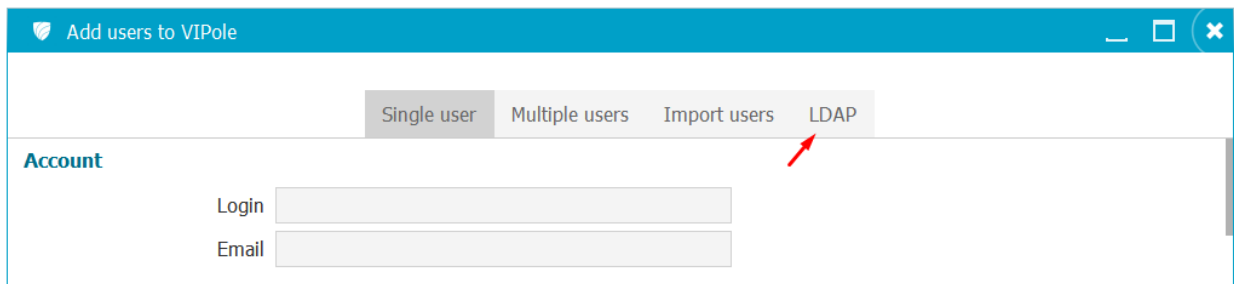
--mapping - setting fields matching when importing the LDAP database and the internal database of VIPole server users. While importing, you can fill the following fields in VIPole database: login, name1, name2, name3, email, nickname, comments.

For example, **--mapping comments=description** sets the matching between the attribute value **description** of the LDAP database and the field **comments** of the database of VIPole server users.

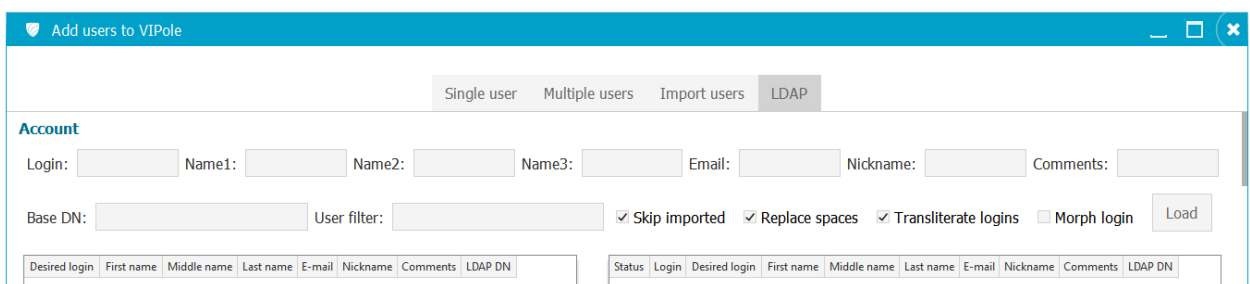
To specify the correspondence of several fields, you need to use several **--mapping** parameters.

Import of users via the «VIPole Administrator» extension of the client application.

Open the LDAP tab.



The LDAP import window will open



The fields «Login», «First name», «Middle name», «Last name», «E-mail», «Nickname », «Comments » are designed for mapping. Here you can enter the names of the LDAP database fields that will be imported to the corresponding fields of the inner database of VIPole server users.

«Base DN» - the DN, from which the search of users is started. If not specified – then the value of the **ldap-users-search-base** parameter of VIPole server configuration file is used.

«User filter» - the filter of user accounts according to which the selection is performed.

For detailed syntax and examples: [Active Directory: LDAP Syntax Filters](#).

«Skip imported» - Do not import existing users.

«Replace spaces» - the spaces in the field will be replaced with underscores.


«Transliterate logins» - the field with Cyrillic characters will be replaced with Latin characters through transliteration.

«Morph login» - in the case of login duplication, a unique number is added to the end of this login.

To import users, filling the «Base DN» field is required. After clicking «Upload», the list of users from the LDAP appears in the table on the left. If the fields in the table are filled incorrectly, change the mapping, specifying attribute names corresponding to your

LDAP database template in the fields «First name», «Middle name», «Last name», «E-mail », «Nickname», «Comments».

Select the users you want to import to VIPole clicking on them:

- Click+Ctrl selects several lines.
- Click+Shift selects a range of rows.
- Using  move the records to the right table.

After clicking «Apply», the list of users from the table on the left will be imported to VIPole database.

The «Generate keys» option allows to generate the encryption keys for the imported user. The password and the secret phrase are generated automatically. The administrator can view them in the Security tab of the «VIPole user administration» window.

During the import, security templates and contact list templates can be applied to users, they are chosen before clicking «Apply».

Export of users from AD/LDAP to a CSV file using the vipole-ldap console utility.

If you specify the **csv-file arg** parameter for vipole-ldap console utility, data will be exported to a CSV file.

With this option, the **--dry-run** option is automatically turned on. Thus, users are not imported to the database. All other parameters work like in the case when the data is imported to the VIPole database.

If necessary, a CSV file can be edited and then imported to the VIPole database using the «VIPole Administrator» extension of the desktop client application.

Note, that in various implementations of AD/LDAP (including AD in different versions of Windows Server) different schemes of naming attributes are used.

Before importing users, make sure that data being imported complies to the fields where it is imported.

If you import users to the VIPole database, first perform the vipole-ldap utility with the **--dry-run** parameter and by the program log check that the desired users are imported and additional fields are filled in correctly.

To view the LDAP database schema, the attribute names, etc. you can use [LDAP Admin](#) or similar programs.

An example of importing new users from AD vipole.ldap.sample .

The search is performed among all users whose usernames begin with testuser (e.g. testuser04 or testusername). Users are imported as testuser04@vipole.ldap.

```
vipole-ldap \  
--admin-password 1234567890 \  
--base-dn CN=Users,DC=vipole,DC=ldap,DC=sample \  
--certificate /etc/vipole/cacert.pk \  
--domain vipole.ldap \  
--login sd_admin --passwd 12345678 \  
--server-host 192.168.1.175  
--filter "(CN=testuser*)"
```

Export of users to a CSV file, with the transfer of the «description» attribute value from a record in LDAP to the «comments» field of VIPole user database and whose login ends with a number that is more than 31 (e.g. testuser_41 or testuser_55).

```
vipole-ldap --admin-password 1234567890 \  
--base-dn OU=OfficeInSPB,DC=vipole,DC=ldap,DC=sample\  
--certificate /etc/vipole/cacert.pk \  
--domain vipole.ldap \  
--login sd_admin \  
--passwd 12345678 \  
--server-host 192.168.1.175 \  
--server-port 37210 \  
--filter "(CN>=testuser_31)" \  
--mapping comments=description \  

```

```
--csv-file ldap-users.csv
```

6. User Connection Logs window

In this window, you can view connections and disconnections of the members of your Security domain, the IP address and the version of the client.

User connections logs

Refresh

Reset filters

	Time	Login	Event	Code	IP address	Session ID	OS	OS version
Filters	All time		Any	Any				
1	2016.08.05 12:34:15	annaschmidt	Logged in	OK	192.168.1.192	57a45d9774e0ba2acac30504	Windows	7
2	2016.08.05 12:34:15	felixfisher	Logged in	OK	192.168.1.168	57a45d9774e0ba2acac30505	Windows	7
3	2016.08.05 12:34:15	annaschmidt	Logged out		192.168.1.192	57a45af674e0ba2acac304e4		
4	2016.08.05 12:34:15	felixfisher	Logged out		192.168.1.168	57a45b2274e0ba2acac304ed		
5	2016.08.05 12:23:46	felixfisher	Logged in	OK	192.168.1.168	57a45b2274e0ba2acac304ed	Windows	7
6	2016.08.05 12:23:02	annaschmidt	Logged in	OK	192.168.1.126	57a45af674e0ba2acac304e4	Windows	7
7	2016.08.05 12:18:30	annaschmidt	Logged out		192.168.1.126	57a42aaf74e0ba2acac304bf		
8	2016.08.05 12:18:30	felixfisher	Logged out		192.168.1.168	57a454b574e0ba2acac304cb		
9	2016.08.05 11:56:21	felixfisher	Logged in	OK	192.168.1.168	57a454b574e0ba2acac304cb	Windows	7
10	2016.08.05 08:57:03	annaschmidt	Logged in	OK	192.168.1.126	57a42aaf74e0ba2acac304bf	Windows	7
11	2016.08.05 08:56:49	annaschmidt	Logged out		192.168.1.126	57a424ba74e0ba2acac304a7		
12	2016.08.05 08:31:38	annaschmidt	Logged in	OK	192.168.1.126	57a424ba74e0ba2acac304a7	Windows	7
13	2016.08.05 08:31:24	annaschmidt	Logged out		192.168.1.126	57a3811b74e0ba2acac30494		
14	2016.08.04 20:53:31	annaschmidt	Logged in	OK	192.168.1.126	57a3811b74e0ba2acac30494	Windows	7
15	2016.08.04 20:53:17	annaschmidt	Logged out		192.168.1.126	57a3774c74e0ba2acac30473		
16	2016.08.04 20:11:40	annaschmidt	Logged in	OK	192.168.1.126	57a3774c74e0ba2acac30473	Windows	7
17	2016.08.04 19:25:12	fernandogarcia	Logged out		192.168.1.126	57a36b0dd0bfd8a535a7f84e		
18	2016.08.04 19:19:25	fernandogarcia	Logged in	OK	192.168.1.126	57a36b0dd0bfd8a535a7f84e	Windows	7
19	2016.08.04 19:19:23	fernandogarcia	Logged out		192.168.1.126	57a36b06d0bfd8a535a7f84a		
20	2016.08.04 19:19:18	fernandogarcia	Logged in	OK	192.168.1.126	57a36b06d0bfd8a535a7f84a	Windows	7
21	2016.08.04 19:18:32	fernandogarcia	Logged out		192.168.1.126	57a36ac8d0bfd8a535a7f845		
22	2016.08.04 19:18:16	fernandogarcia	Logged in	OK	192.168.1.126	57a36ac8d0bfd8a535a7f845	Windows	7
23	2016.08.04 19:17:55	felixfisher	Logged in	OK	192.168.1.168	57a36ab3d0bfd8a535a7f842	Windows	7
24	2016.08.04 19:17:53	felixfisher	Logged out		192.168.1.168	57a36aacd0bfd8a535a7f83e		
25	2016.08.04 19:17:48	felixfisher	Logged in	OK	192.168.1.168	57a36aacd0bfd8a535a7f83e	Windows	7

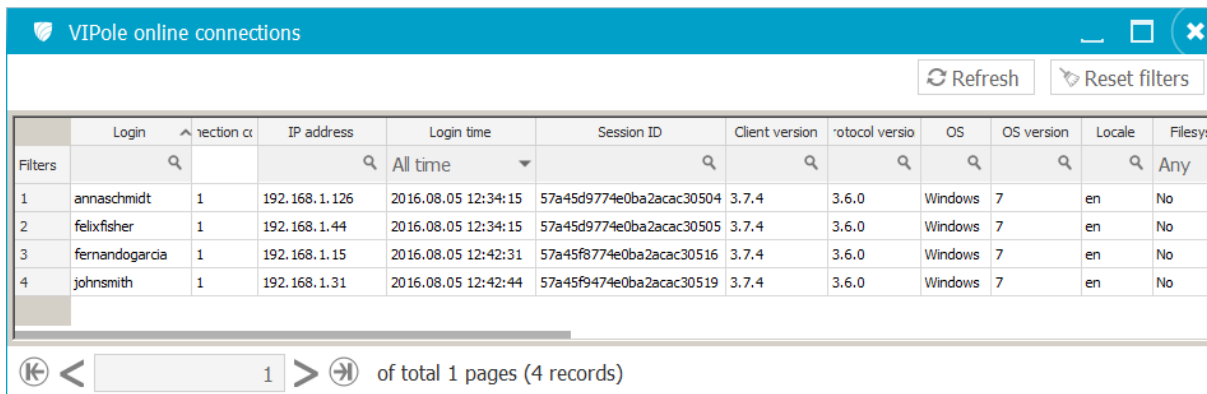
<

1

>

of total 2 pages (35 records)

7. Online Connection window



The screenshot shows a window titled "VIPole online connections". It features a "Refresh" button and a "Reset filters" button. Below these is a table with columns: Login, Connection ID, IP address, Login time, Session ID, Client version, Protocol version, OS, OS version, Locale, and Filesystem. The table contains four rows of data. At the bottom, there is a pagination bar showing "1" of total 1 pages (4 records).

	Login	Connection ID	IP address	Login time	Session ID	Client version	Protocol version	OS	OS version	Locale	Filesystem
1	annaschmidt	1	192.168.1.126	2016.08.05 12:34:15	57a45d9774e0ba2acac30504	3.7.4	3.6.0	Windows	7	en	No
2	felixfisher	1	192.168.1.44	2016.08.05 12:34:15	57a45d9774e0ba2acac30505	3.7.4	3.6.0	Windows	7	en	No
3	fernandogarcia	1	192.168.1.15	2016.08.05 12:42:31	57a45f8774e0ba2acac30516	3.7.4	3.6.0	Windows	7	en	No
4	johnsmith	1	192.168.1.31	2016.08.05 12:42:44	57a45f9474e0ba2acac30519	3.7.4	3.6.0	Windows	7	en	No

In this window, you can view a list of the members of your Security domain who are currently online. If there are several active sessions, all of them will be shown. You can view the IP address of your computer, the version of the operating system, the client version and whether the file system on the user's computer is encrypted.