



The Dude

Sistema de monitoreo

Potente, practico y gratuito

<https://mikrotik.com/thedude>



David Vega

Analista de seguridad informática

Cisco CCNA Cyber Ops - Security Analyst Nessus - ISO/IEC 27001

www.davenisc.com

Historia:

- Inicios en 2004 hasta 2009 en Apartado Antioquia **PSSPC** taller de mantenimiento.
- Luego en 2010 hasta 2018 en Bogotá **NISC** (Network Integration Services Colombia) Licenciamiento y Telecomunicaciones
- Actualmente 2019 en Bogotá **DaveNISC** Analista de seguridad informática, licenciamiento, telecomunicaciones, hacking ético, programación, asesorías, charlas, entre otros.

2019



Dave**NISC**
Expertos en seguridad informática

2010 - 2018



2004 - 2009





3
Países



36
Clientes

Agenda

1. Ventajas the-dude
2. Instalación en Windows y Linux
3. Interfaz web
4. ¿Que se puede monitorear con the-dude?
5. Sistema de alertas
6. Notificaciones con Telegram

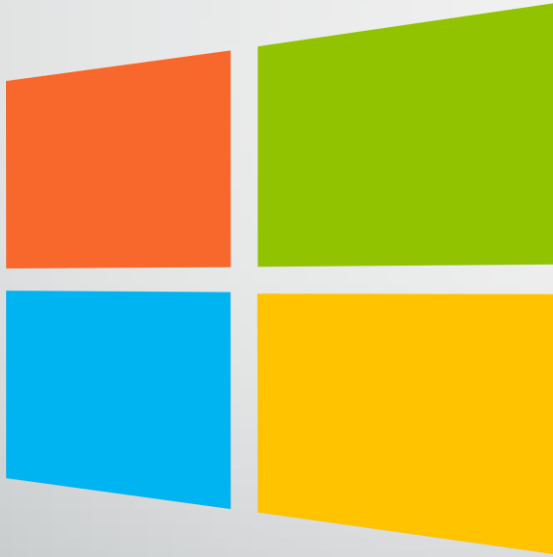
Sistema de monitoreo con The Dude

Ventajas:

1. Fácil integración con RB Mikrotik
2. Instalación en Windows o Linux
3. Interfaz web
4. Monitoreo en tiempo real
5. Sistema de alertas



Instalación



Sistemas recomendados
Windows 10 y 7



Sistemas recomendados
Ubuntu y Debian

Requisitos del sistema

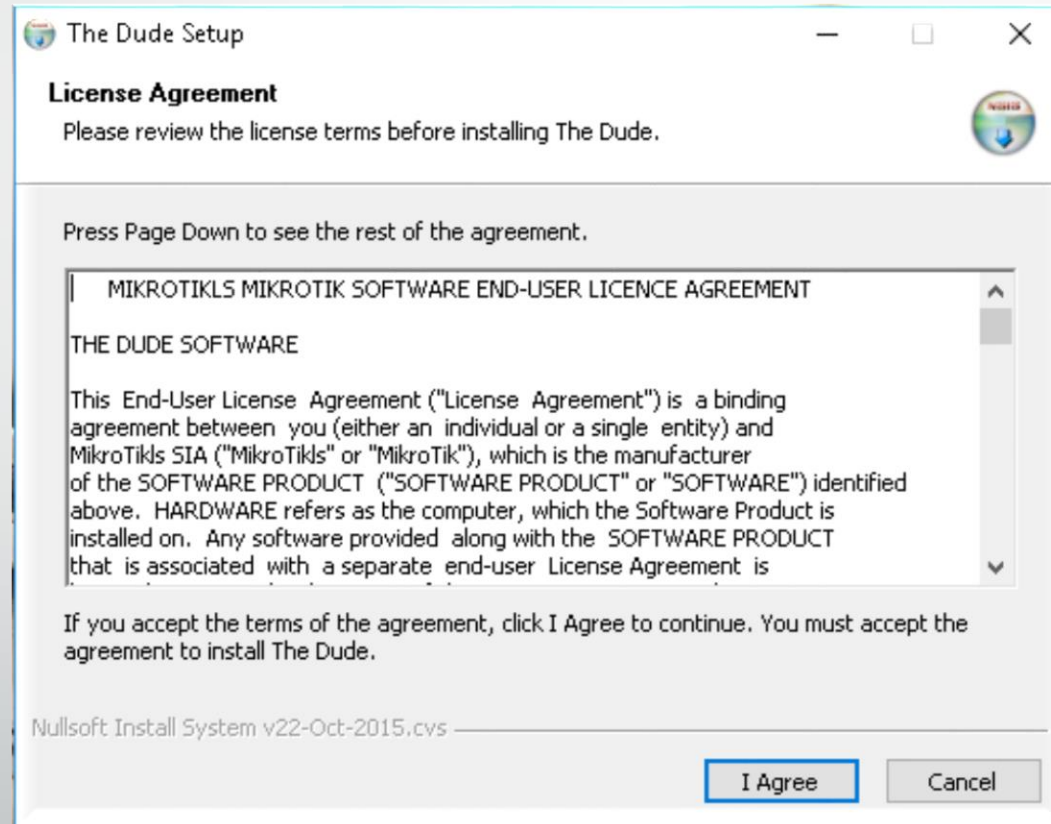
RouterOS:

- v6.34rc13 o superior

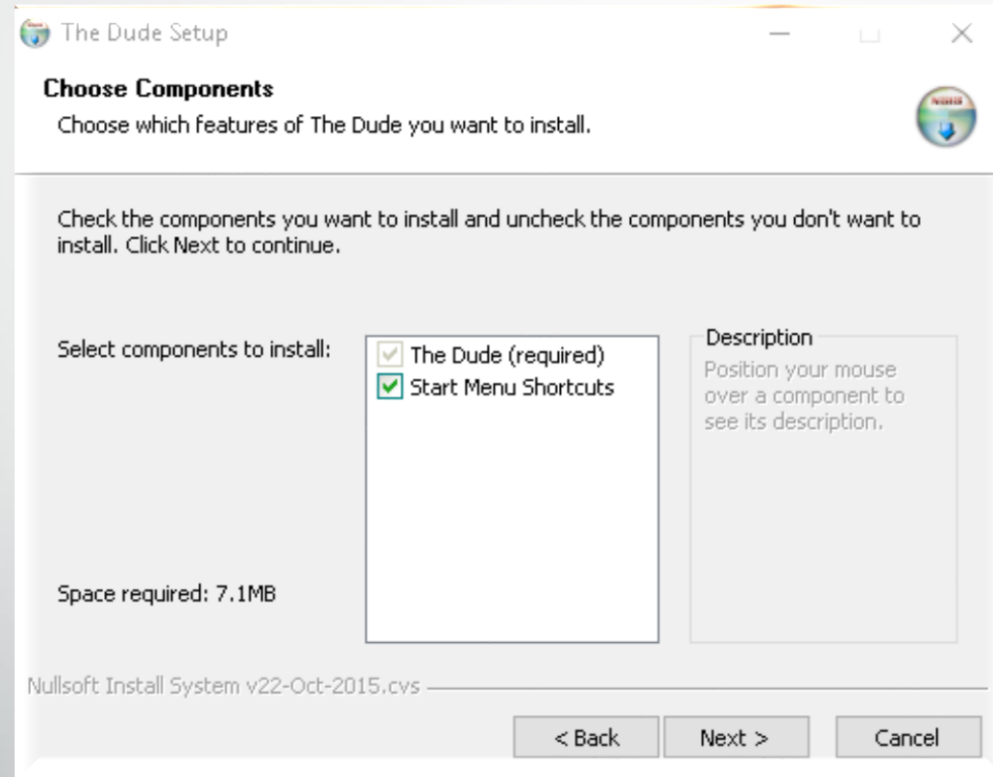
Hardware:

- TILE devices;
- ARM devices;
- MMIPS devices;
- RouterOS x86 installations;
- RouterOS [CHR environment](#)
- NO con SMIPS → hAP mini y hAP lite

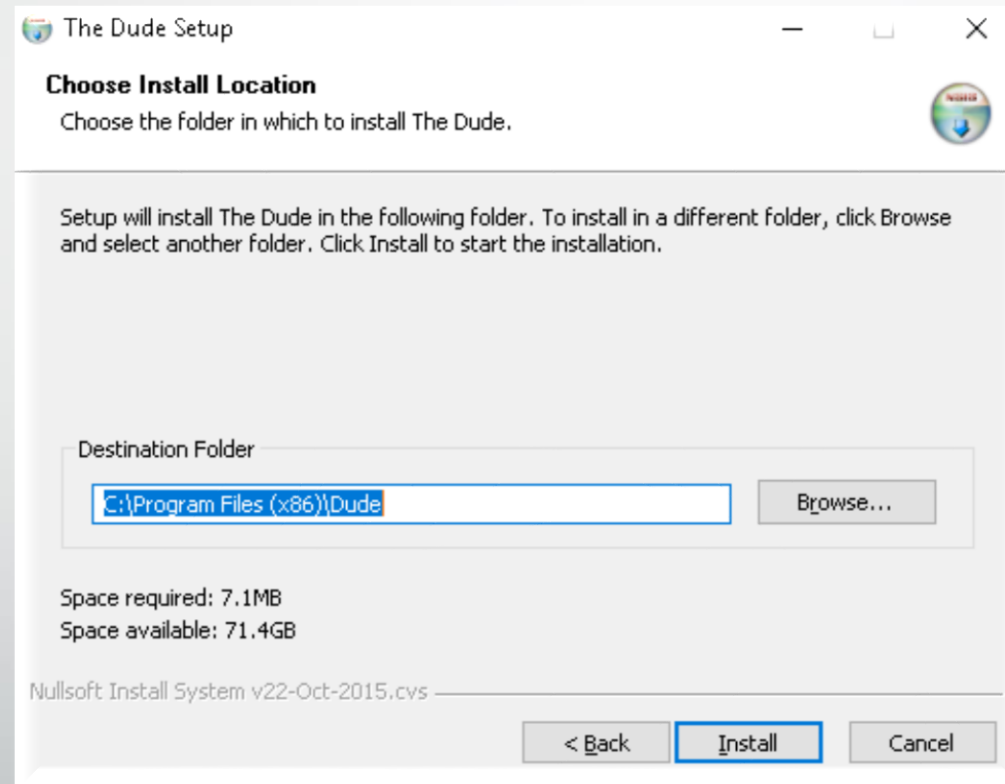
Instalación en Windows



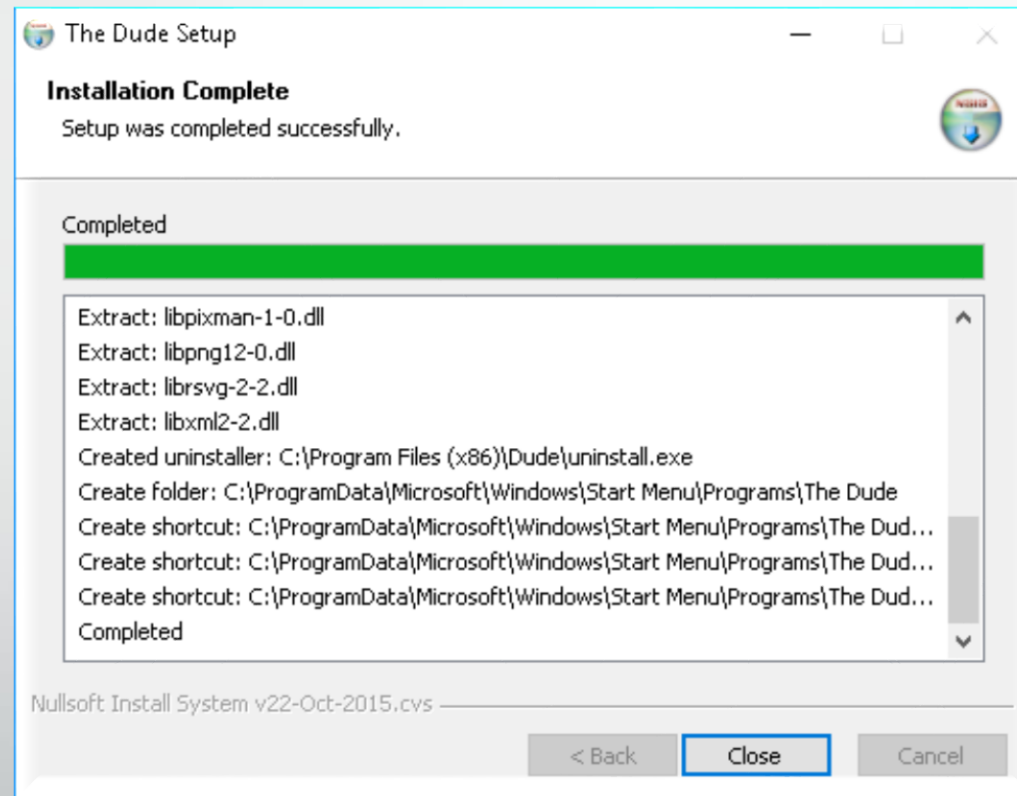
Instalación en Windows



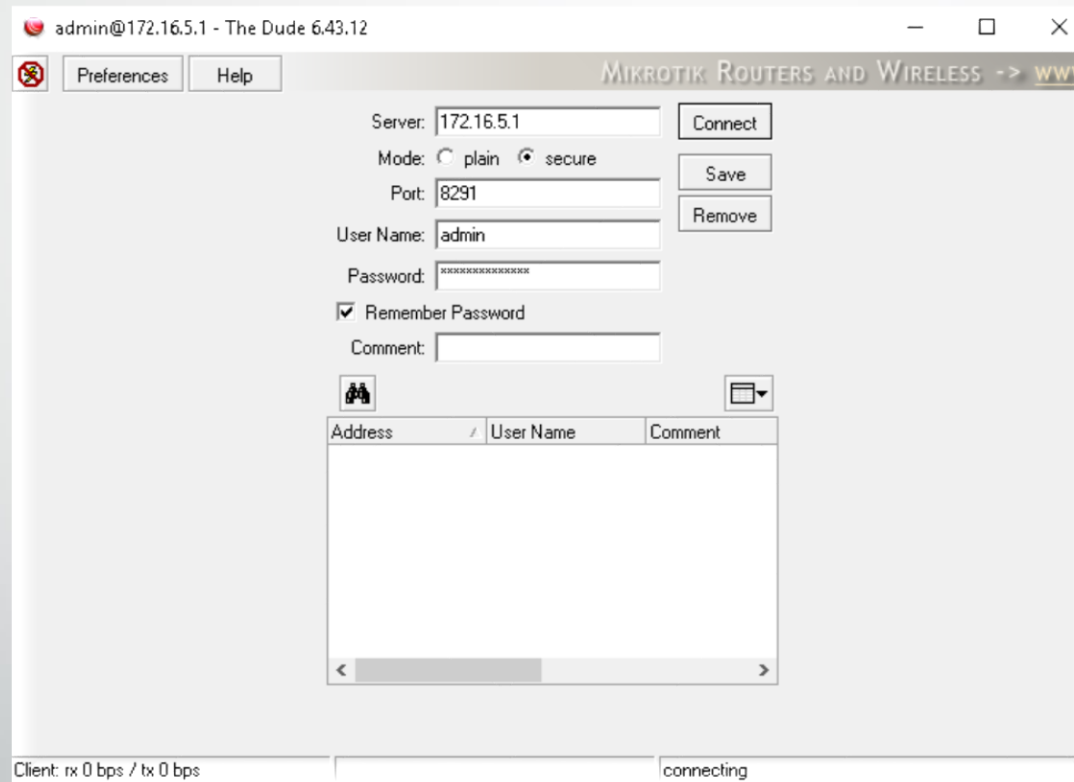
Instalación en Windows



Instalación en Windows



Instalación en Windows



Instalación en Windows

The screenshot shows the main interface of The Dude 6.34rc15. The window title is "krisjanis@172.16.0.254 - The Dude 6.34rc15". The interface includes a menu bar with "Preferences" and "Help", and a toolbar with "Settings", "CSU", and other icons. The "Contents" pane on the left lists various categories like Address Lists, Admins, Charts, Devices, Files, Functions, History Actions, Links, Logs, Network Maps, Networks, Notifications, Panels, Probes, and Services. The "Tools" table is displayed in the center-right, listing various tools and their associated devices.

Name	Device
Bandwidth Test	all
Dude	all
Ftp	all
Ping	all
Remote Connection	all
Scan	all
Snmwalk	all
Spectral Scan	all
Telnet	all
Terminal	all
Torch	all
Traceroute	all
Web	all
Winbox	all

The screenshot shows the main interface of The Dude 6.34rc45. The window title is "admin@gateway.lan - The Dude 6.34rc45". The interface includes a menu bar with "Preferences" and "Help", and a toolbar with "Settings", "Discover", and "Tools". The "Contents" pane on the left lists various categories like Address Lists, Admins, Agents, Charts, Devices, Files, Functions, History Actions, Links, Logs, Network Maps, Networks, Notifications, Panels, Probes, and Services. The main area displays a network diagram with various nodes and connections. The status bar at the bottom shows "Client: rx 6.4 kbps / tx 248 bps" and "Server: rx ...".

Instalación en Linux



Instalación de wine en Ubuntu

- 1) Agregamos el soporte a la arquitectura de 64 bits.

→ `sudo dpkg --add-architecture i386`

- 2) Agregamos la clave de verificación.

→ `wget -nc https://dl.winehq.org/wine-builds/Release.key`

→ `sudo apt-key add Release.key`

Instalación wine

- 3) Agregamos el repositorio.

→ Ubuntu: `sudo apt-add-repository https://dl.winehq.org/wine-builds/ubuntu/`

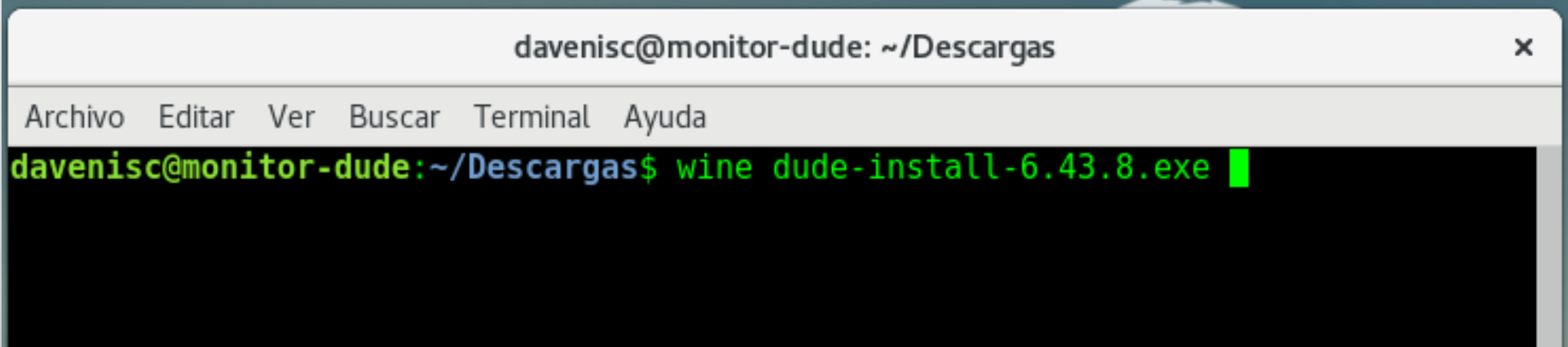
- 4) Actualizamos

→ `sudo apt update`

Instalación wine

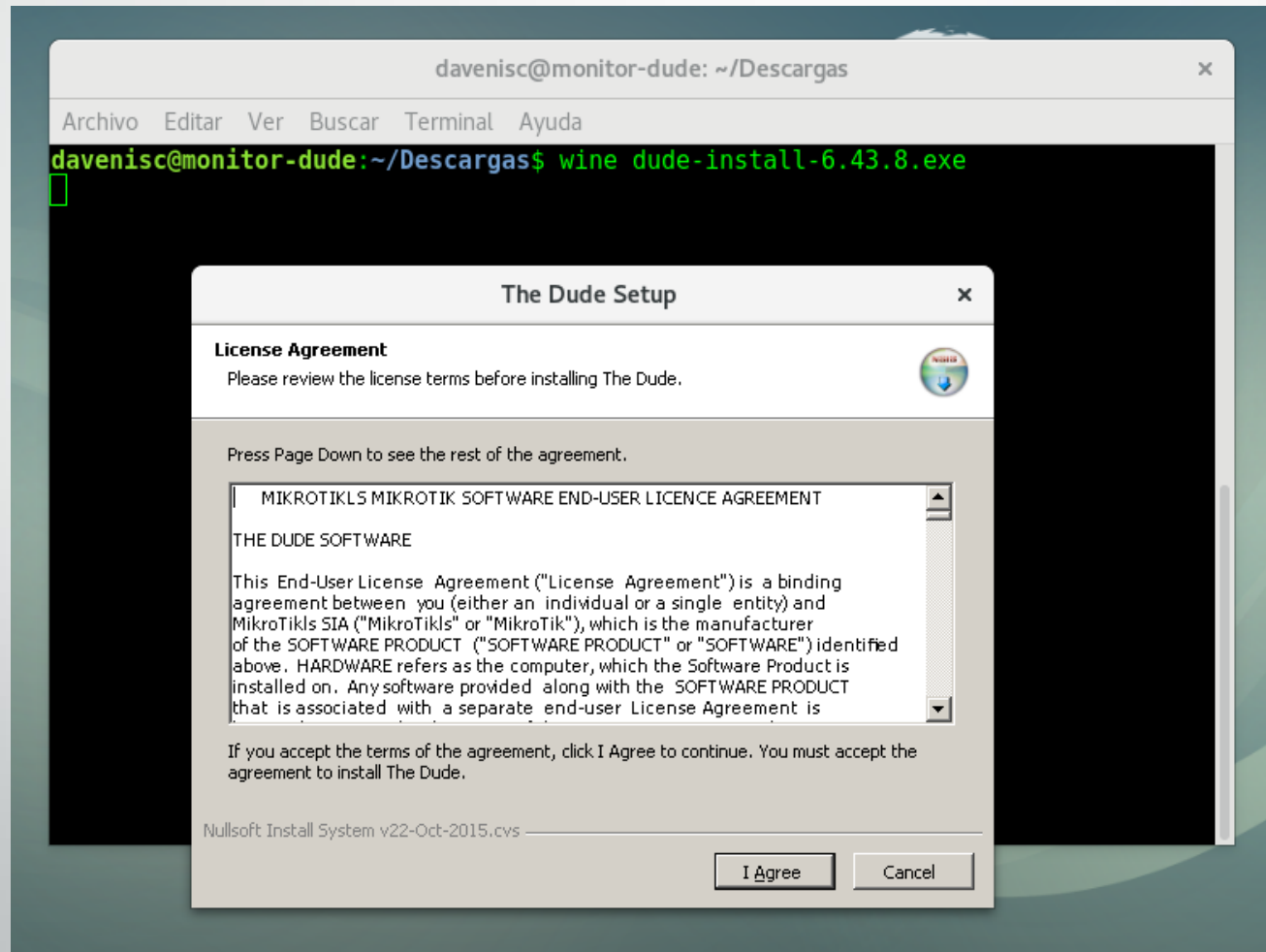
- 5) Instalamos la versión estable:
→ `sudo apt install --install-recommends winehq-stable`
- 6) Corregimos errores de instalación
→ `sudo apt-get install -f`

Instalación dude con wine

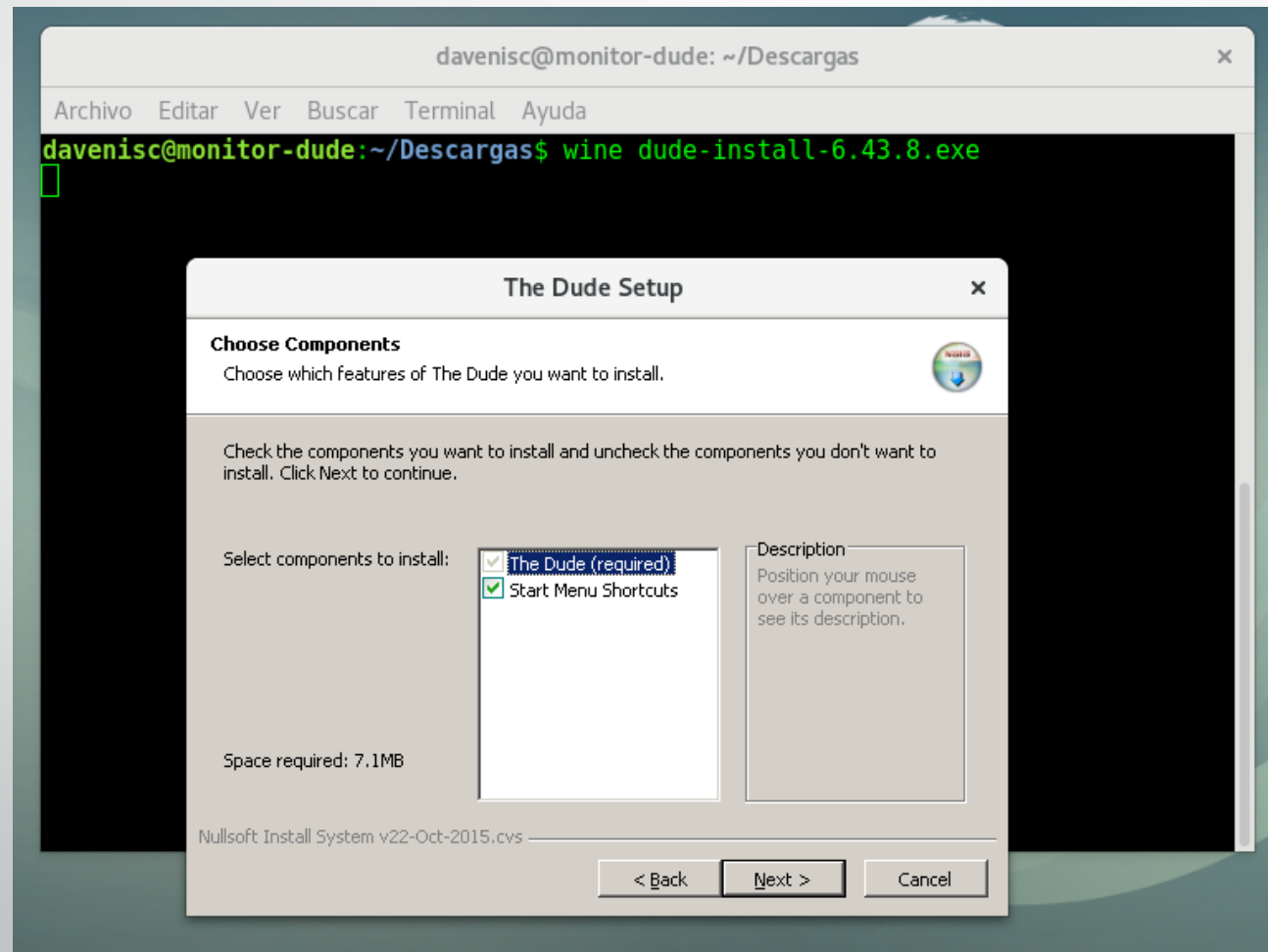
A terminal window titled "davenisc@monitor-dude: ~/Descargas" with a close button (x) in the top right corner. The window has a menu bar with "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The terminal content shows the command "davenisc@monitor-dude:~/Descargas\$ wine dude-install-6.43.8.exe" followed by a green cursor.

```
davenisc@monitor-dude: ~/Descargas  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
davenisc@monitor-dude:~/Descargas$ wine dude-install-6.43.8.exe █
```

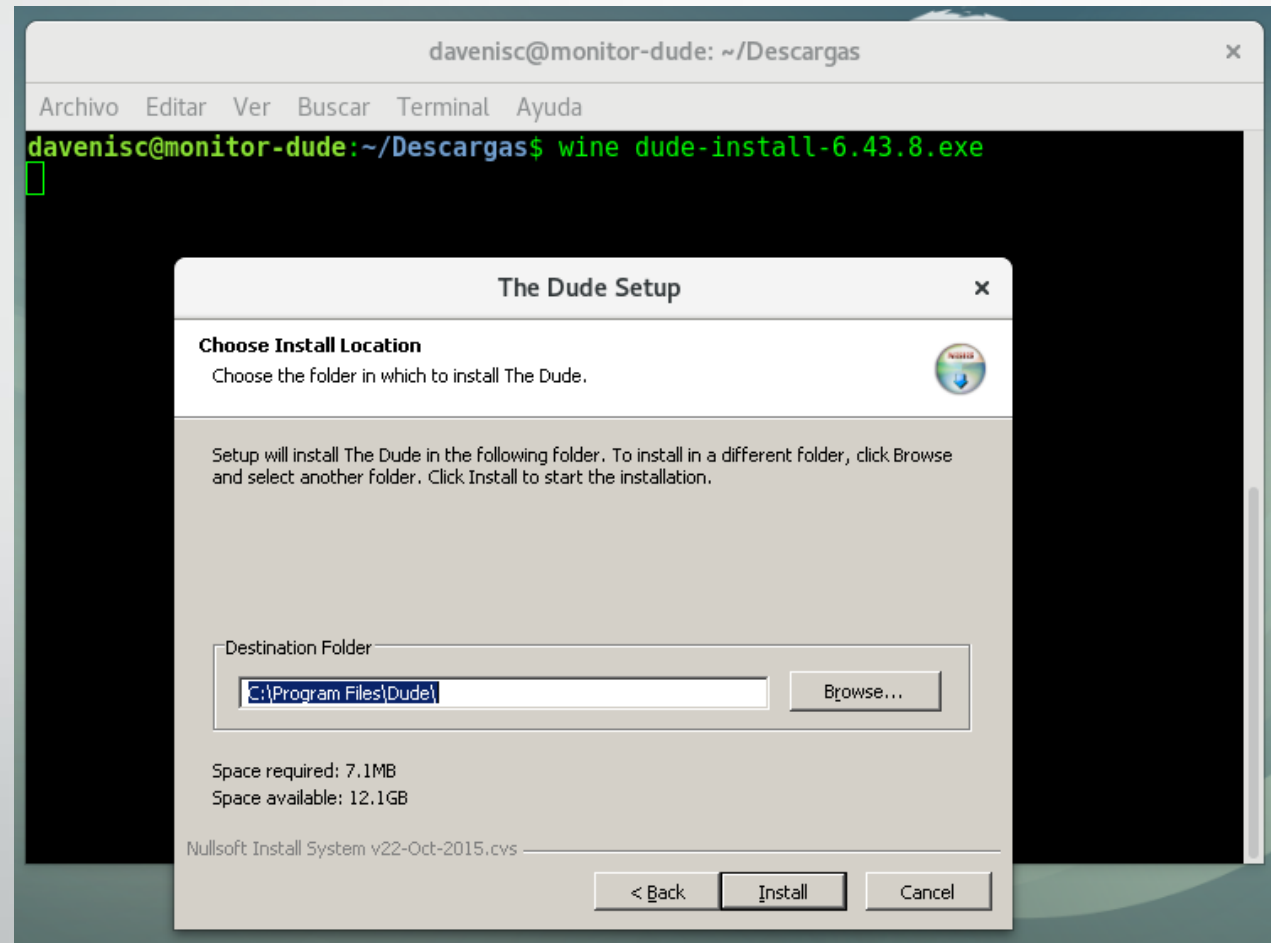
Instalación dude con wine



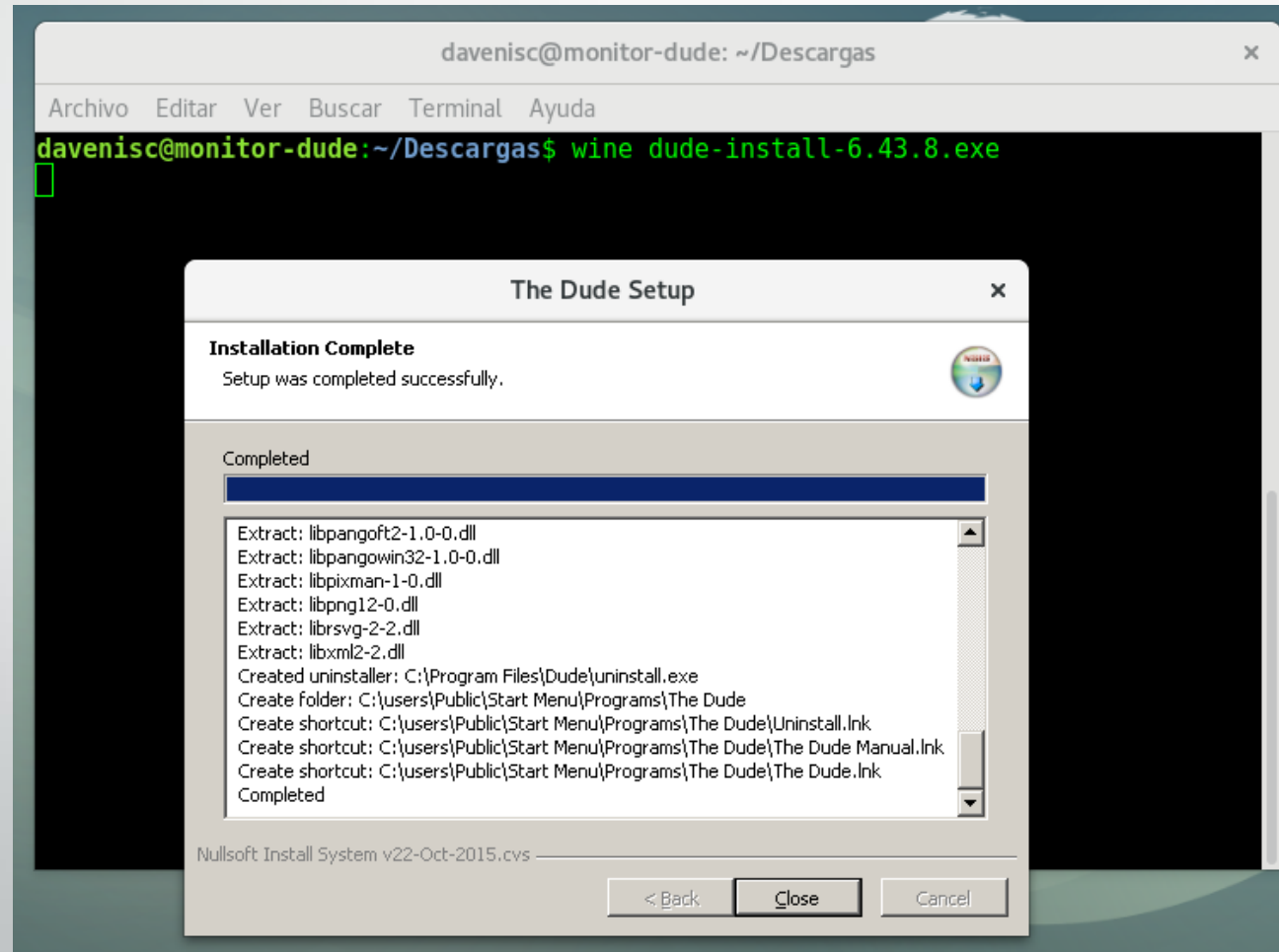
Instalación dude con wine



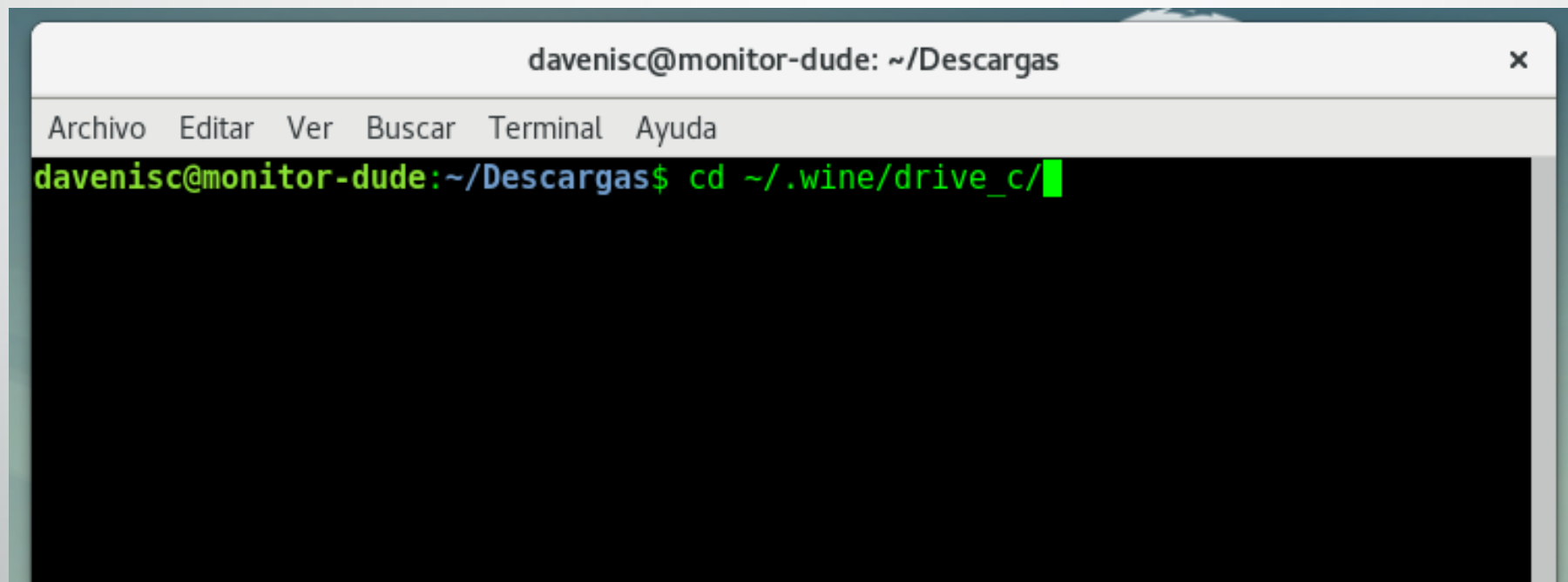
Instalación dude con wine



Instalación dude con wine

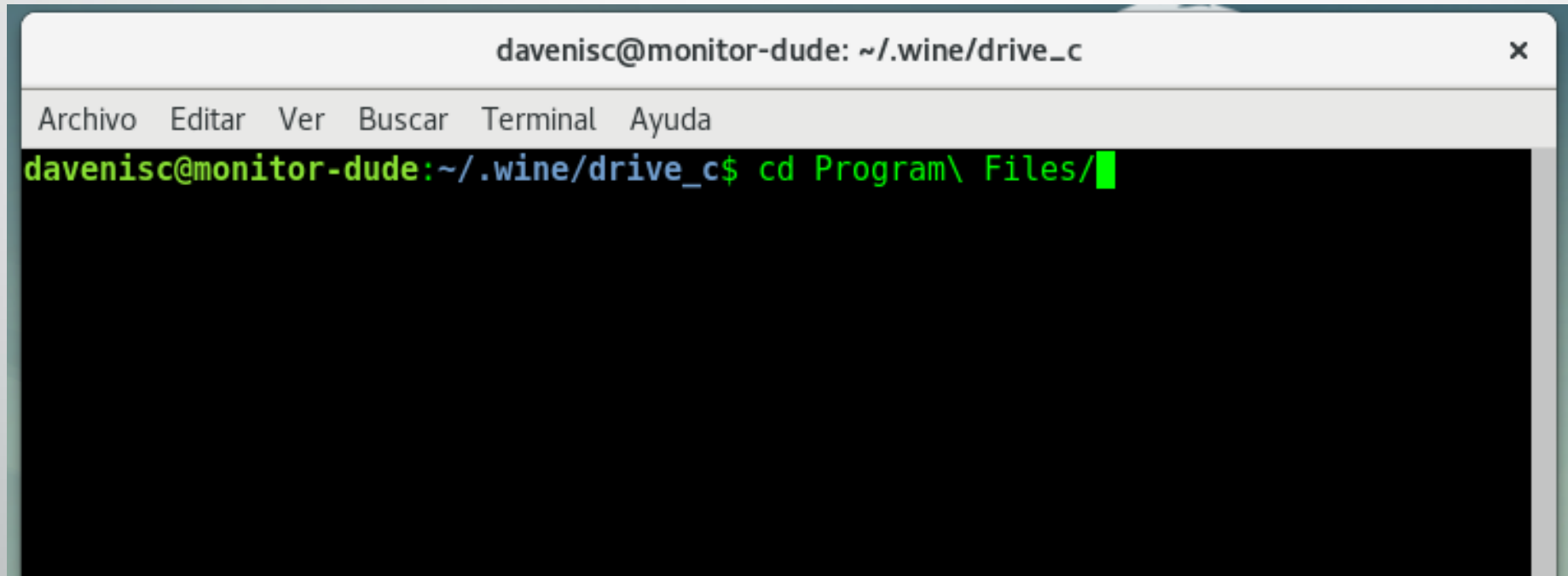


Entrar a la carpeta wine

A terminal window with a title bar that reads "davenisc@monitor-dude: ~/Descargas" and a close button "x". Below the title bar is a menu bar with the items "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The main area of the terminal is black with green text. The prompt "davenisc@monitor-dude:~/Descargas\$" is followed by the command "cd ~/.wine/drive_c/" and a green cursor.

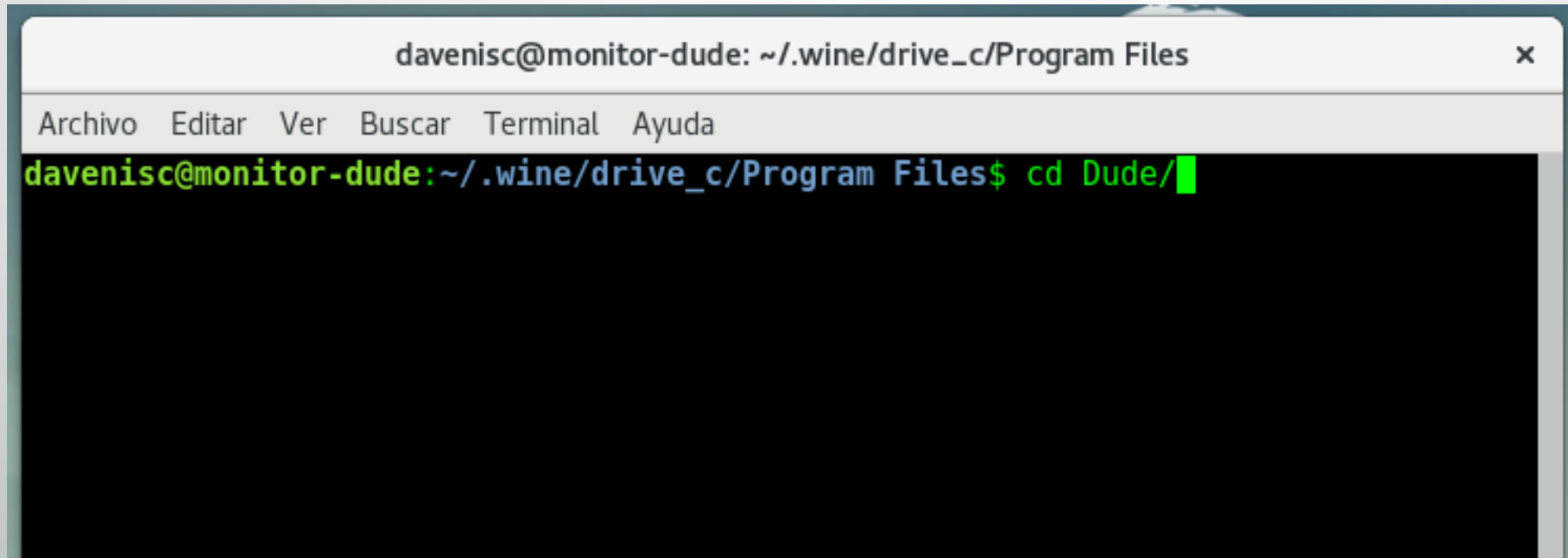
```
davenisc@monitor-dude: ~/Descargas  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
davenisc@monitor-dude:~/Descargas$ cd ~/.wine/drive_c/
```


Entrar a Program\ Files/

A terminal window with a title bar that reads "davenisc@monitor-dude: ~/.wine/drive_c" and a close button "x". Below the title bar is a menu bar with the items "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The main area of the terminal is black and contains the text "davenisc@monitor-dude:~/.wine/drive_c\$ cd Program\ Files/" in green, with a green cursor at the end of the line.

```
davenisc@monitor-dude: ~/.wine/drive_c  
Archivo  Editar  Ver  Buscar  Terminal  Ayuda  
davenisc@monitor-dude:~/.wine/drive_c$ cd Program\ Files/
```

Entrar a la carpeta Dude/

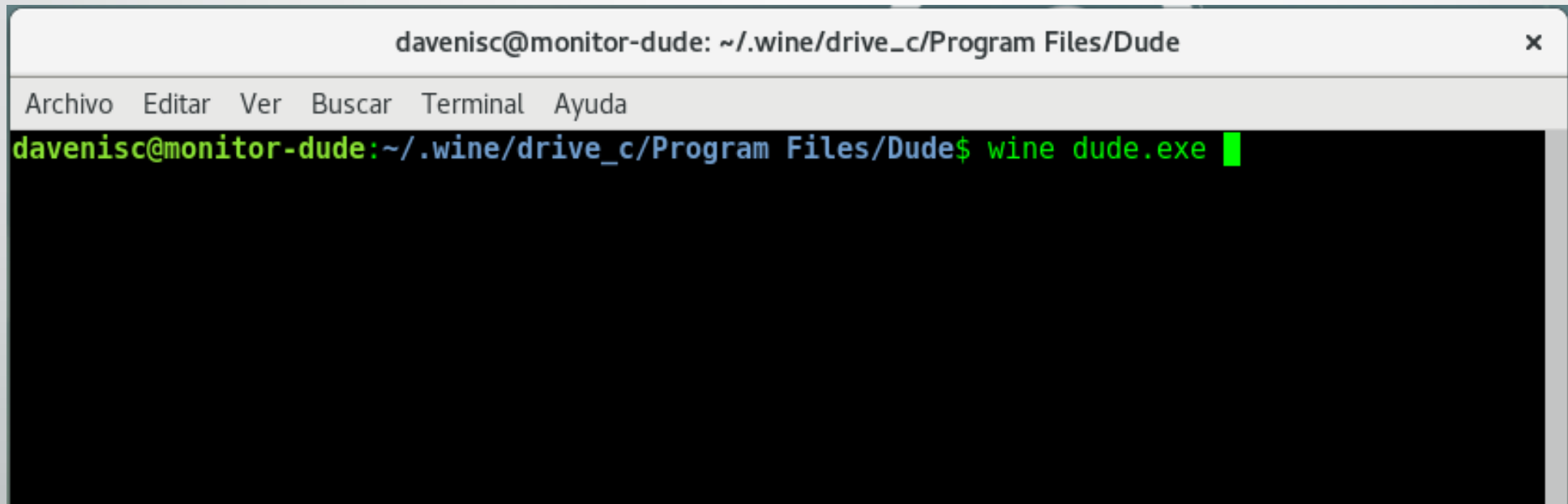
A terminal window with a title bar that reads "davenisc@monitor-dude: ~/.wine/drive_c/Program Files" and a close button. Below the title bar is a menu bar with the options "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The main area of the terminal is black with green text. The prompt "davenisc@monitor-dude:~/.wine/drive_c/Program Files\$" is followed by the command "cd Dude/" and a green cursor.

```
davenisc@monitor-dude: ~/.wine/drive_c/Program Files
Archivo  Editar  Ver     Buscar  Terminal  Ayuda
davenisc@monitor-dude:~/.wine/drive_c/Program Files$ cd Dude/
```

Listar archivos ls -l

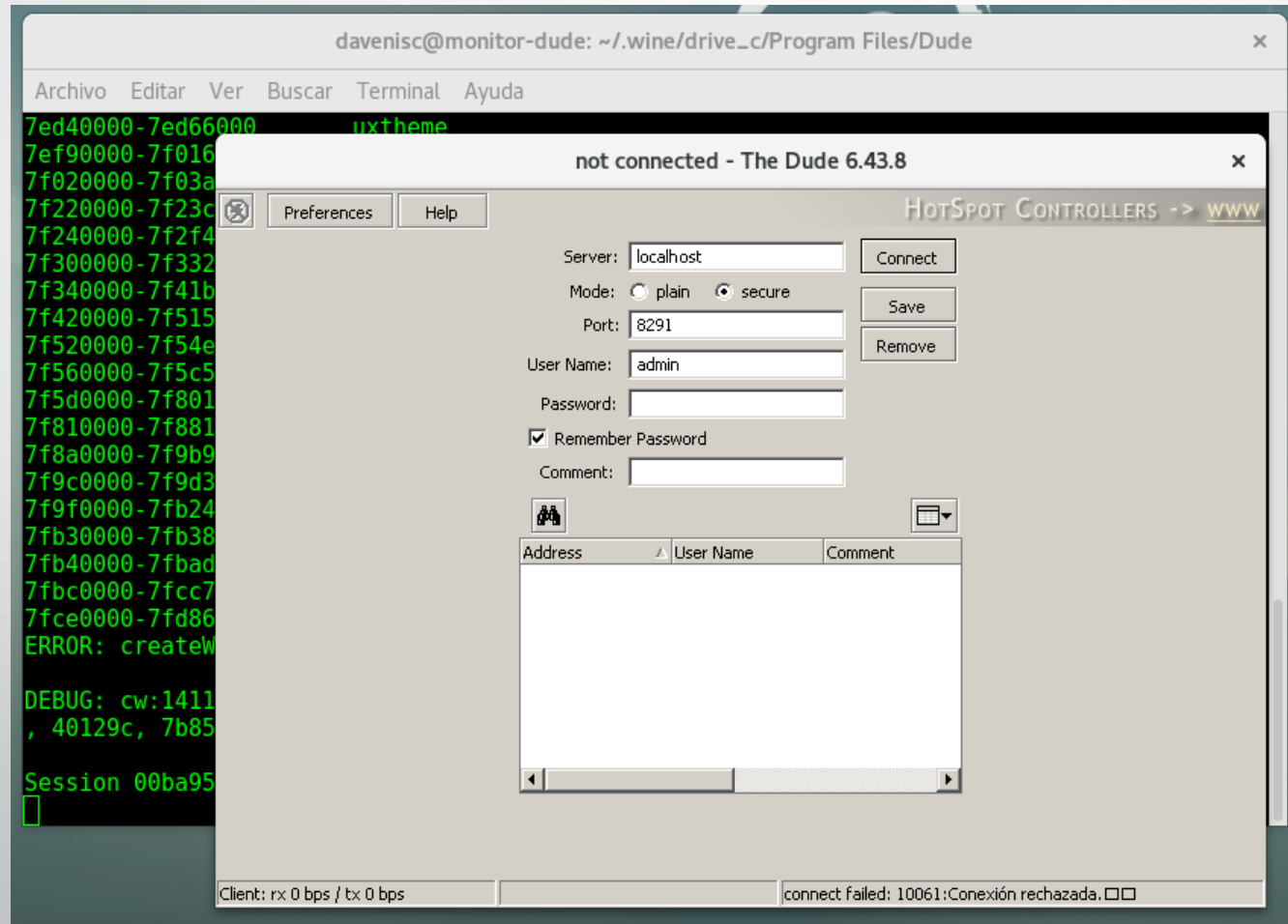
```
davenisc@monitor-dude: ~/.wine/drive_c/Program Files/Dude x
Archivo Editar Ver Buscar Terminal Ayuda
davenisc@monitor-dude:~/.wine/drive_c/Program Files/Dude$ ls -l
total 7412
drwxr-xr-x 3 davenisc davenisc  4096 ene 30 18:10 data
-rwxr-xr-x 1 davenisc davenisc 3714048 dic 21 02:19 dude.exe
drwxr-xr-x 2 davenisc davenisc  4096 ene 30 18:10 language
-rw-r--r-- 1 davenisc davenisc  367616 dic 21 02:19 libcairo-2.dll
-rw-r--r-- 1 davenisc davenisc  171520 dic 21 02:19 libcroco-0.6-3.dll
-rw-r--r-- 1 davenisc davenisc  102912 dic 21 02:19 libexpat-1.dll
-rw-r--r-- 1 davenisc davenisc  138240 dic 21 02:19 libfontconfig-1.dll
-rw-r--r-- 1 davenisc davenisc  380928 dic 21 02:19 libfreetype-6.dll
-rw-r--r-- 1 davenisc davenisc  119808 dic 21 02:19 libgdk_pixbuf-2.0-0.dll
-rw-r--r-- 1 davenisc davenisc  257024 dic 21 02:19 libgio-2.0-0.dll
-rw-r--r-- 1 davenisc davenisc  738816 dic 21 02:19 libglib-2.0-0.dll
-rw-r--r-- 1 davenisc davenisc   14336 dic 21 02:19 libgmodule-2.0-0.dll
-rw-r--r-- 1 davenisc davenisc  173056 dic 21 02:19 libgobject-2.0-0.dll
-rw-r--r-- 1 davenisc davenisc  116224 dic 21 02:19 libjpeg-62.dll
-rw-r--r-- 1 davenisc davenisc  199680 dic 21 02:19 libpango-1.0-0.dll
-rw-r--r-- 1 davenisc davenisc   35840 dic 21 02:19 libpangocairo-1.0-0.dll
-rw-r--r-- 1 davenisc davenisc  121344 dic 21 02:19 libpangoft2-1.0-0.dll
-rw-r--r-- 1 davenisc davenisc   38400 dic 21 02:19 libpangowin32-1.0-0.dll
-rw-r--r-- 1 davenisc davenisc  141312 dic 21 02:19 libpixman-1-0.dll
-rw-r--r-- 1 davenisc davenisc  173056 dic 21 02:19 libpng12-0.dll
-rw-r--r-- 1 davenisc davenisc  180736 dic 21 02:19 librsvg-2-2.dll
-rw-r--r-- 1 davenisc davenisc  284160 dic 21 02:19 libxml2-2.dll
-rwxr-xr-x 1 davenisc davenisc  72859 feb 21 15:54 uninstall.exe
davenisc@monitor-dude:~/.wine/drive_c/Program Files/Dude$ █
```

Ejecutar dude con wine

A terminal window with a title bar that reads "davenisc@monitor-dude: ~/.wine/drive_c/Program Files/Dude" and a close button "x". The menu bar contains "Archivo", "Editar", "Ver", "Buscar", "Terminal", and "Ayuda". The main content area shows the command "davenisc@monitor-dude:~/.wine/drive_c/Program Files/Dude\$ wine dude.exe" followed by a green cursor. The rest of the terminal area is black.

```
davenisc@monitor-dude: ~/.wine/drive_c/Program Files/Dude
Archivo Editar Ver Buscar Terminal Ayuda
davenisc@monitor-dude:~/.wine/drive_c/Program Files/Dude$ wine dude.exe
```

The dude con wine



Interfaz web

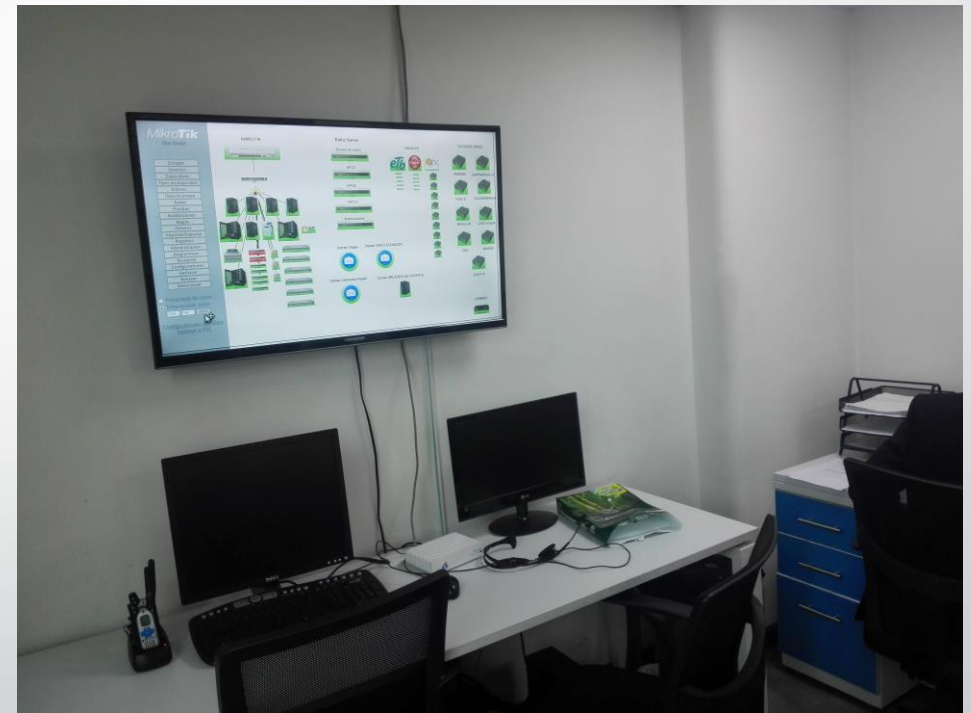
The image shows a configuration window for a web interface. The window is titled "Interfaz web" and contains several settings:

- Remoto:** A dropdown menu.
- Acceso Web:** A section with a checked checkbox labeled "Habilitar".
- Puerto:** A text input field containing "80".
- Puerto seguro:** A text input field containing "443".
- Redes permitidas:** A text input field containing "0.0.0.0/0".
- Excedido tiempo de sesion:** A dropdown menu containing "00:15:00".
- Intervalo de refresco:** A dropdown menu containing "00:00:30".
- Certificate:** A dropdown menu containing "certificate.pem", with a small icon to its left and a "..." button to its right.

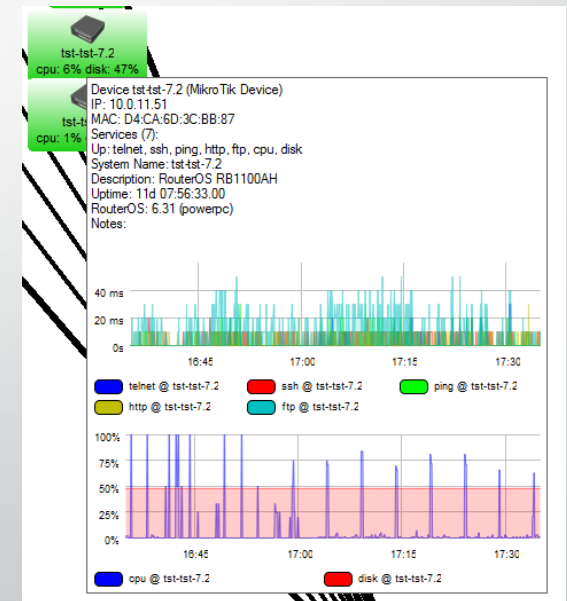
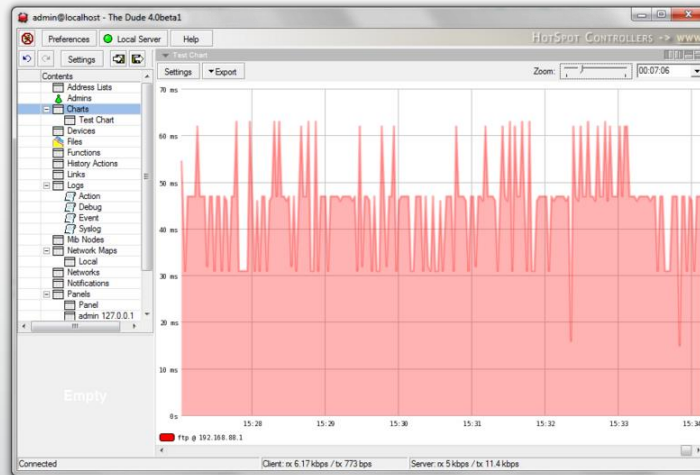
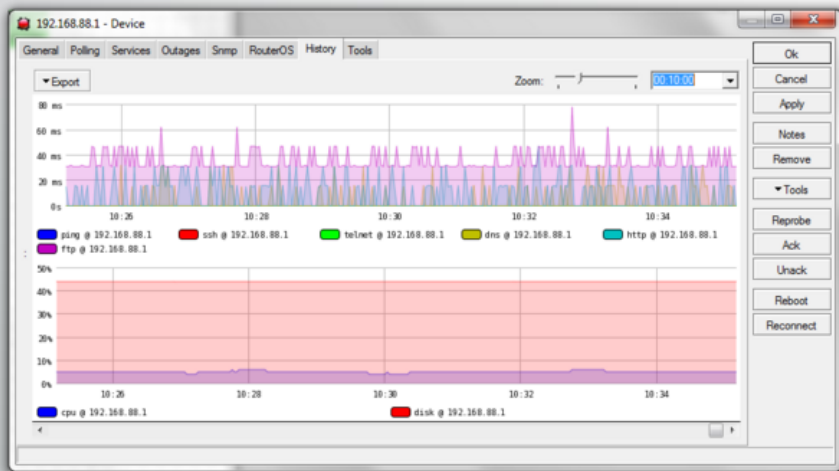
On the right side of the window, there are two buttons: "Aplicar" and "Puesta a cero".

At the bottom of the window, there is a status bar with three indicators: "Conectado", "Client: rx 0 bps / tx 0 bps", and "Servidor: rx 0 bps / tx 0 bps".

Interfaz web



Monitoreo en tiempo real



Sistema de alertas

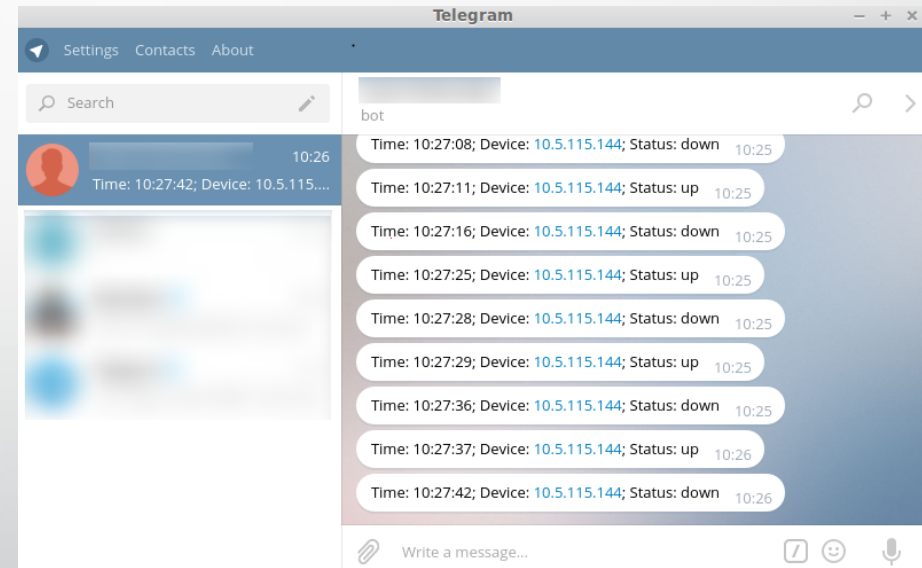
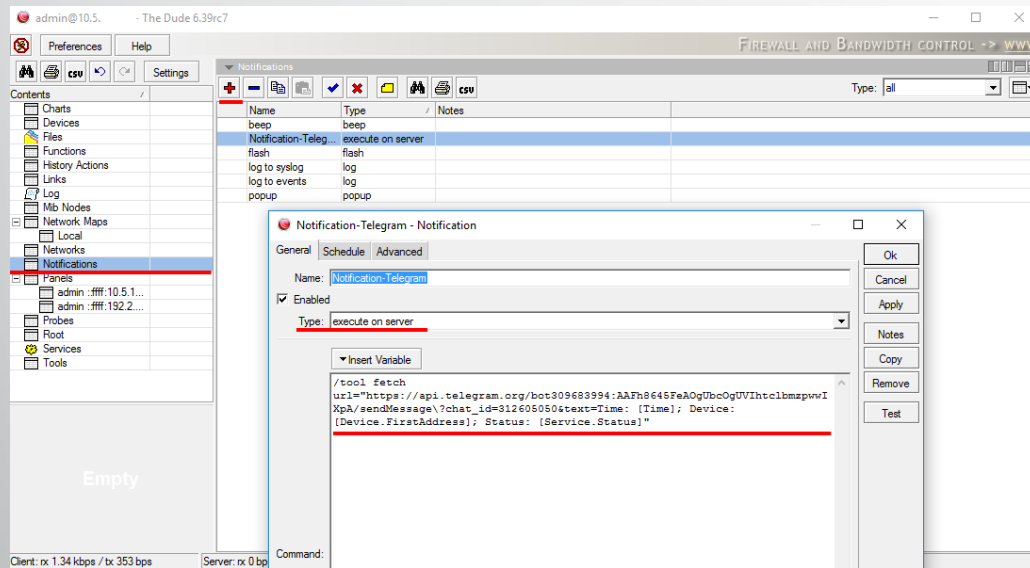


Alertas
Correo electrónico



Alertas
Telegram

Notificaciones con Telegram



https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Dude_Telegram_Example

Notificaciones con Telegram

APIs de telegramas

Ofrecemos dos tipos de API para desarrolladores. El [Bot API](#) le permite crear fácilmente programas que usan mensajes de Telegram para una interfaz. La [API de Telegram y TDLib](#) le permiten crear sus propios clientes de Telegram personalizados. Le invitamos a utilizar ambas API de forma gratuita.

También puede agregar [Telegram Widgets](#) a su sitio web.

API API

Esta API le permite conectar bots a nuestro sistema. [Los Telegram Bots](#) son cuentas especiales que no requieren un número de teléfono adicional para configurar. Estas cuentas sirven como una interfaz para el código que se ejecuta en algún lugar de su servidor.

Para usar esto, no necesita saber nada sobre cómo funciona nuestro protocolo de cifrado MTProto; nuestro servidor intermediario se encargará de todo el cifrado y la comunicación con la API de Telegram. Se comunica con este servidor a través de una interfaz simple HTTPS que ofrece una versión simplificada de la API de Telegram.


[Obtenga más información sobre la API de Bot aquí »](#)


Los desarrolladores de bot también pueden utilizar nuestra [API de pagos](#) para aceptar **pagos** de usuarios de Telegram en todo el mundo.




Crear Bot con Telegram



Info. del bot



BotFather 
bot

 BotFather is the one bot to rule them all. Use it to create new bot accounts and manage your existing bots.
Descripción

@BotFather
Alias

 Notificaciones 

[ENVIAR MENSAJE](#)

I can help you create and manage Telegram bots. If you're new to the Bot API, please [see the manual](#).

You can control me by sending these commands:

[/newbot](#) - create a new bot
[/mybots](#) - edit your bots [beta]

Edit Bots

[/setname](#) - change a bot's name
[/setdescription](#) - change bot description
[/setabouttext](#) - change bot about info
[/setuserpic](#) - change bot profile photo
[/setcommands](#) - change the list of commands
[/deletebot](#) - delete a bot

Bot Settings

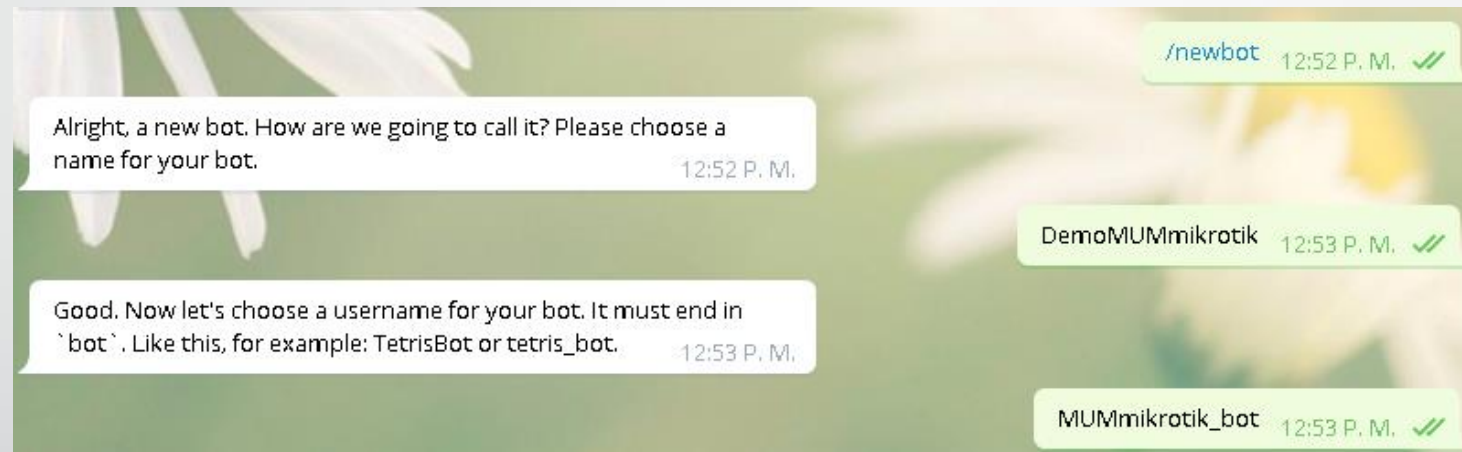
[/token](#) - generate authorization token
[/revoke](#) - revoke bot access token
[/setinline](#) - toggle [inline mode](#)
[/setinlinegeo](#) - toggle [inline location requests](#)
[/setinlinefeedback](#) - change [inline feedback](#) settings
[/setjoingroups](#) - can your bot be added to groups?
[/setprivacy](#) - toggle [privacy mode](#) in groups

Games

[/mygames](#) - edit your [games](#) [beta]
[/newgame](#) - create a new [game](#)
[/listgames](#) - get a list of your [games](#)
[/editgame](#) - edit a [game](#)
[/deletegame](#) - delete an existing [game](#)

12:49 P. M.

Crear Bot con Telegram



Token

Done! Congratulations on your new bot. You will find it at t.me/MUMmikrotik_bot. You can now add a description, about section and profile picture for your bot, see [/help](#) for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

Use this token to access the HTTP API:

729185341:AAF0mxQmuiVr3B0tuqASy_0i870tobyq_pM

Keep your token secure and **store it safely**, it can be used by anyone to control your bot.

For a description of the Bot API, see this page:

<https://core.telegram.org/bots/api>



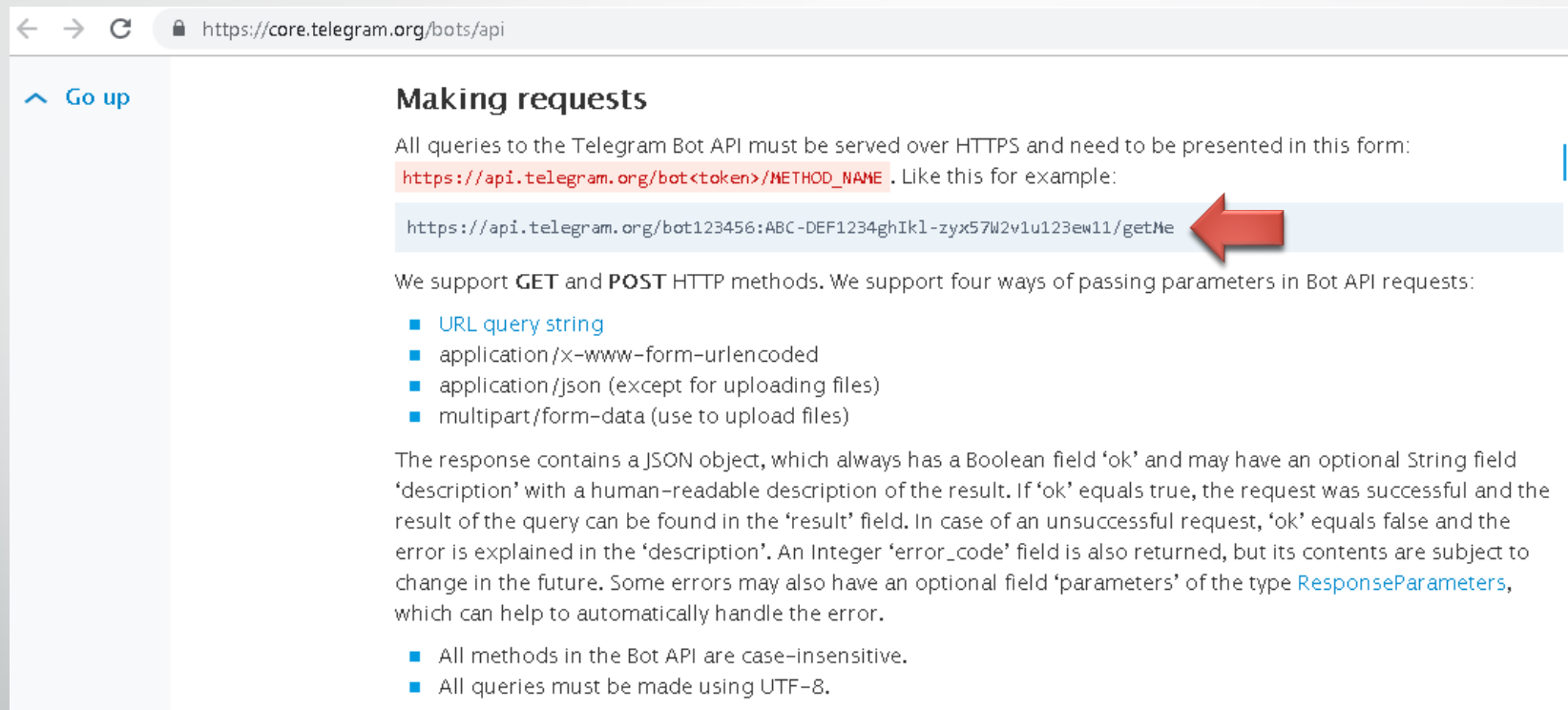
1



2

12:53 P. M.

URL para obtener el ID de grupo



The screenshot shows the Telegram Bot API documentation page. The browser address bar displays `https://core.telegram.org/bots/api`. The page title is "Making requests". The text explains that all queries must be served over HTTPS and provides a template URL: `https://api.telegram.org/bot<token>/METHOD_NAME`. A specific example URL is highlighted in a light blue box: `https://api.telegram.org/bot123456:ABC-DEF1234ghIkl1-zyx57W2v1u123ew11/getMe`. A red arrow points to the `getMe` part of this URL. Below the URL, it states that GET and POST methods are supported and lists four ways to pass parameters: URL query string, application/x-www-form-urlencoded, application/json, and multipart/form-data. The response format is described as a JSON object with fields for 'ok', 'description', 'error_code', and 'parameters'. A final list of notes states that all methods are case-insensitive and queries must be in UTF-8.

Go up

Making requests

All queries to the Telegram Bot API must be served over HTTPS and need to be presented in this form: `https://api.telegram.org/bot<token>/METHOD_NAME`. Like this for example:

```
https://api.telegram.org/bot123456:ABC-DEF1234ghIkl1-zyx57W2v1u123ew11/getMe
```

We support **GET** and **POST** HTTP methods. We support four ways of passing parameters in Bot API requests:

- [URL query string](#)
- `application/x-www-form-urlencoded`
- `application/json` (except for uploading files)
- `multipart/form-data` (use to upload files)

The response contains a JSON object, which always has a Boolean field 'ok' and may have an optional String field 'description' with a human-readable description of the result. If 'ok' equals true, the request was successful and the result of the query can be found in the 'result' field. In case of an unsuccessful request, 'ok' equals false and the error is explained in the 'description'. An Integer 'error_code' field is also returned, but its contents are subject to change in the future. Some errors may also have an optional field 'parameters' of the type [ResponseParameters](#), which can help to automatically handle the error.

- All methods in the Bot API are case-insensitive.
- All queries must be made using UTF-8.

Crear Bot con Telegram

← → ↻ <https://core.telegram.org/bots/api>

[Go up](#)

Making requests

All queries to the Telegram Bot API must be served over HTTPS and need to be presented in this form: `https://api.telegram.org/bot<token>/METHOD_NAME`. Like this for example:

```
https://api.telegram.org/bot123456:ABC-DEF1234ghIk1-zyx57W2v1u123ew11/getMe
```

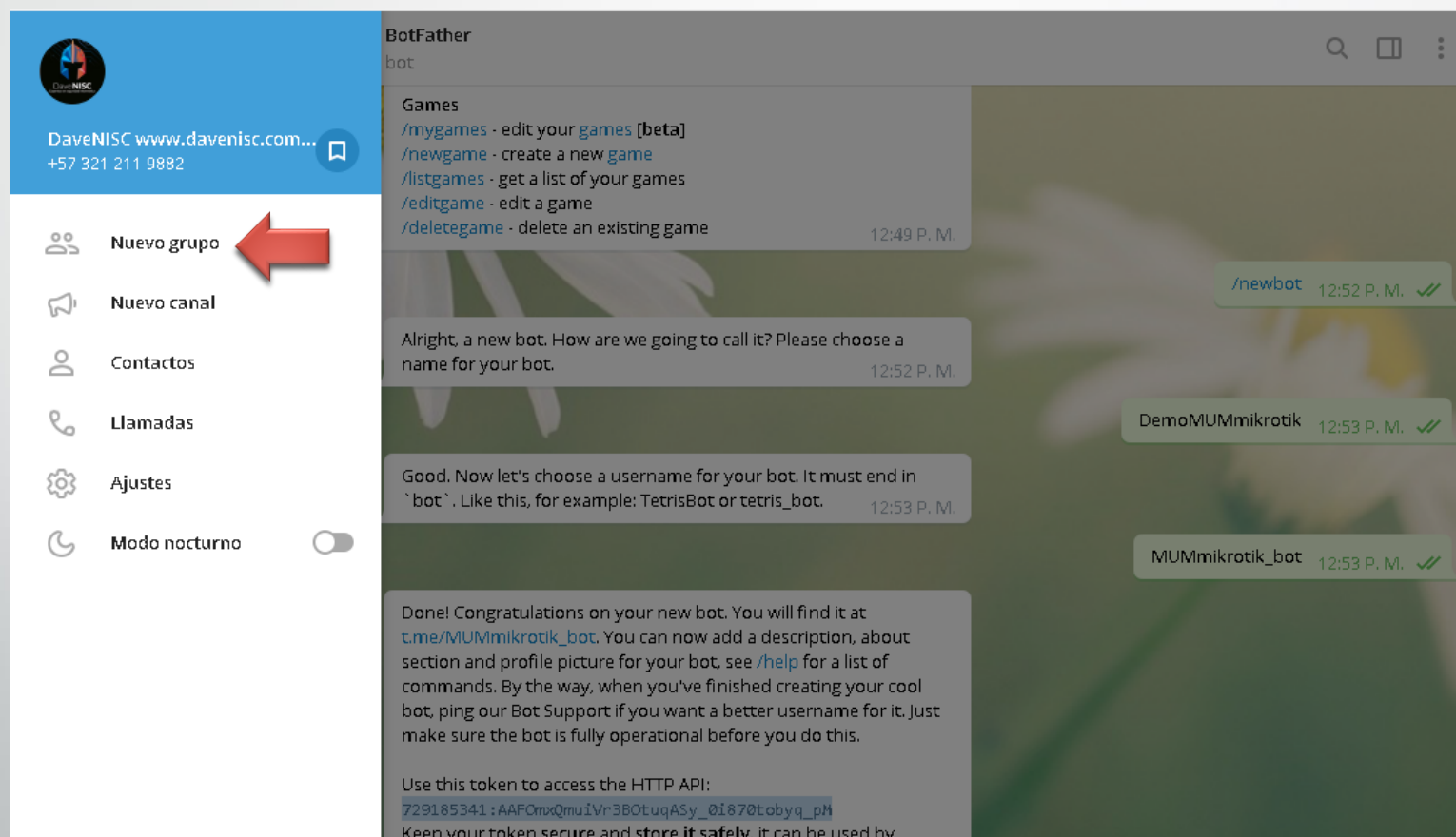
We support **GET** and **POST** HTTP methods. We support four ways of passing parameters in Bot API requests:

- [URL query string](#)
- `application/x-www-form-urlencoded`
- `application/json` (except for uploading files)
- `multipart/form-data` (use to upload files)

The response contains a JSON object, which always has a Boolean field 'ok' and may have an optional String field 'description' with a human-readable description of the result. If 'ok' equals true, the request was successful and the result of the query can be found in the 'result' field. In case of an unsuccessful request, 'ok' equals false and the error is explained in the 'description'. An Integer 'error_code' field is also returned, but its contents are subject to change in the future. Some errors may also have an optional field 'parameters' of the type [ResponseParameters](#), which can help to automatically handle the error.

- All methods in the Bot API are case-insensitive.
- All queries must be made using UTF-8.

Crear un grupo en Telegram



The screenshot displays the Telegram mobile application interface. On the left, a navigation menu is visible with the following options: 'Nuevo grupo' (highlighted with a red arrow), 'Nuevo canal', 'Contactos', 'Llamadas', 'Ajustes', and 'Modo nocturno'. The main chat area shows a conversation with 'BotFather'. The chat history includes a list of commands for a bot named 'Games', a confirmation message for a new bot, a request for a bot name, a request for a bot username, and a final congratulatory message with a token and instructions. The chat area also shows three outgoing messages: '/newbot', 'DemoMUMmikrotik', and 'MUMmikrotik_bot', all of which are marked as read.

Navigation Menu:

- Nuevo grupo
- Nuevo canal
- Contactos
- Llamadas
- Ajustes
- Modo nocturno

BotFather chat:

Games

- /mygames - edit your games [beta]
- /newgame - create a new game
- /listgames - get a list of your games
- /editgame - edit a game
- /deletegame - delete an existing game

Alright, a new bot. How are we going to call it? Please choose a name for your bot.

Good. Now let's choose a username for your bot. It must end in 'bot'. Like this, for example: TetrisBot or tetris_bot.

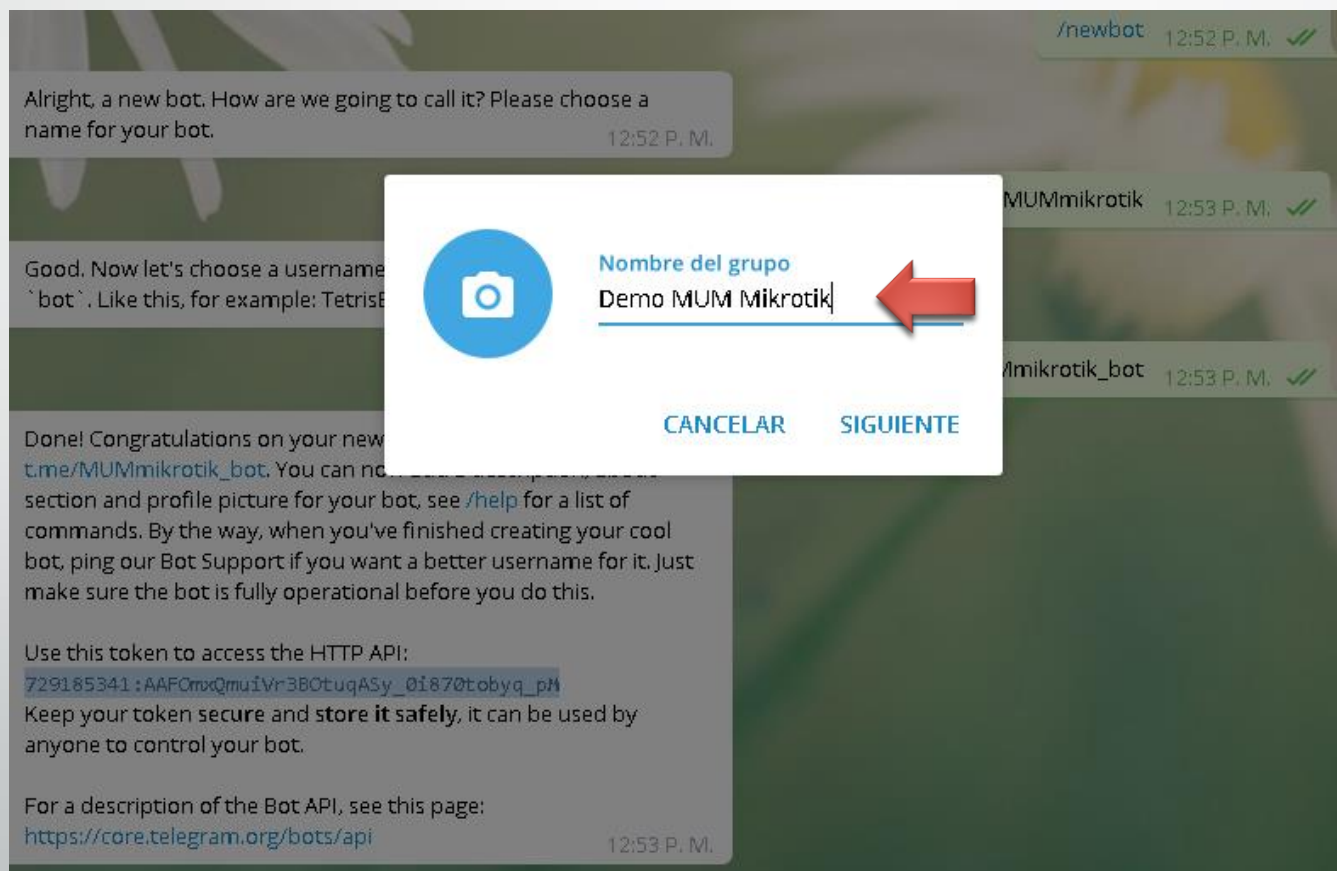
Done! Congratulations on your new bot. You will find it at t.me/MUMmikrotik_bot. You can now add a description, about section and profile picture for your bot, see /help for a list of commands. By the way, when you've finished creating your cool bot, ping our Bot Support if you want a better username for it. Just make sure the bot is fully operational before you do this.

Use this token to access the HTTP API:
`729185341:AAF0mxQmuIVr3BOtuqASy_0i870tobyq_pM`
Keep your token secure and store it safely. it can be used by

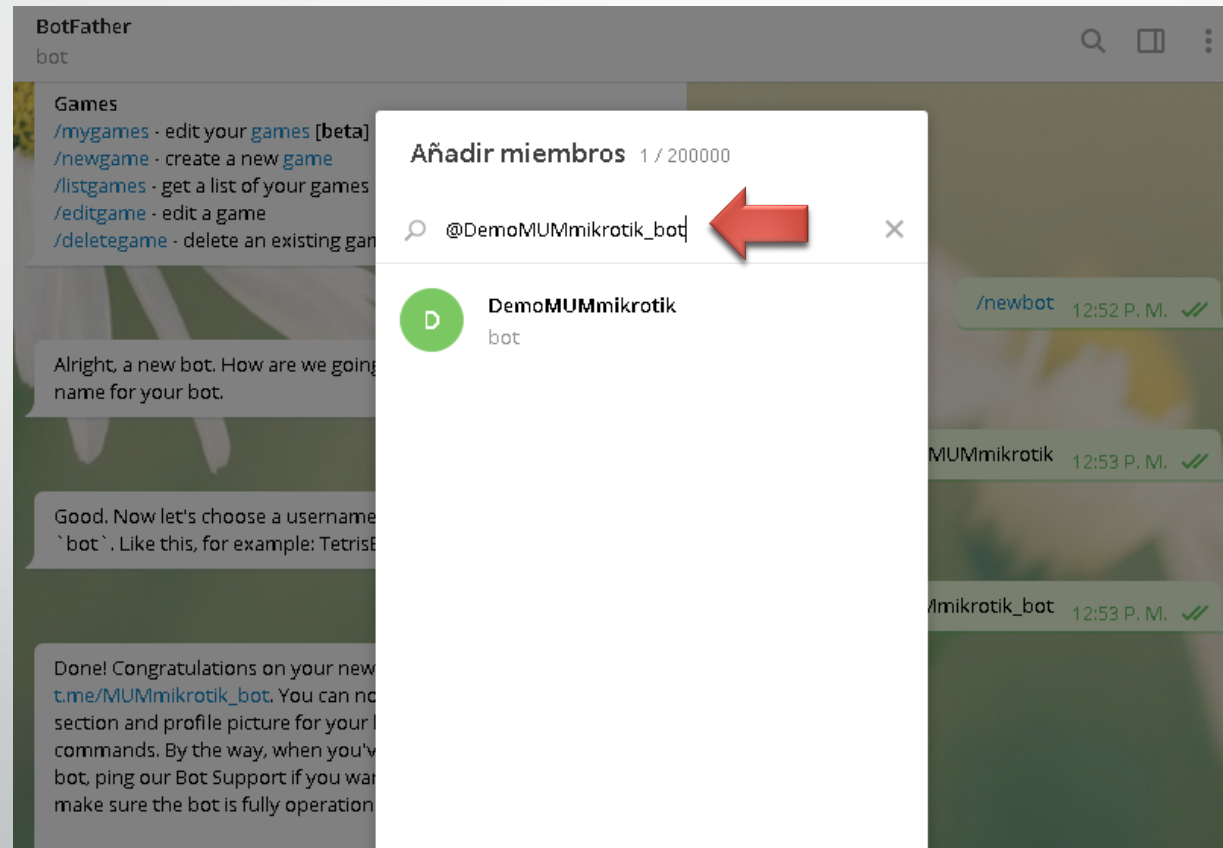
Outgoing messages:

- /newbot
- DemoMUMmikrotik
- MUMmikrotik_bot

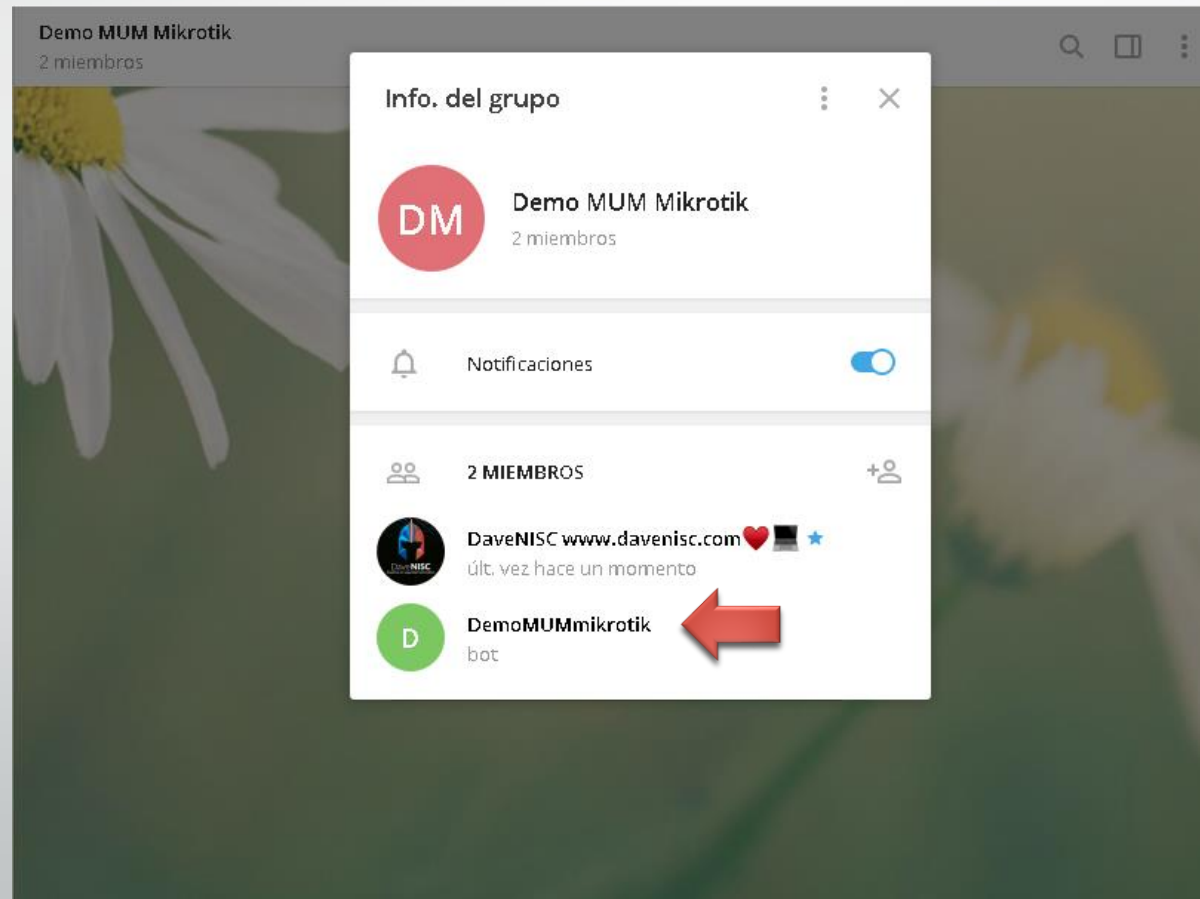
Nombre de grupo



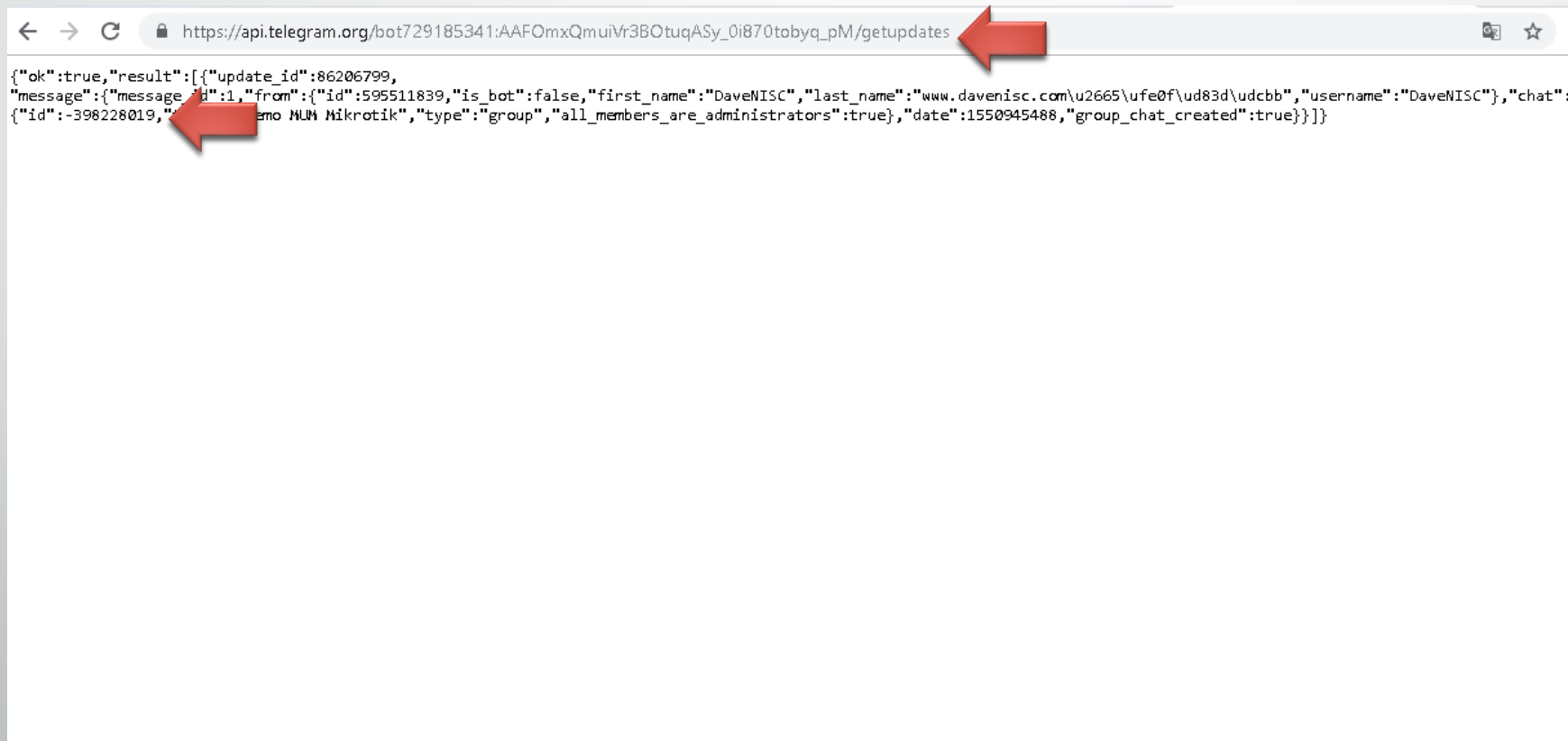
Unir Bot a grupo



Bot en el grupo



Crear Bot con Telegram



```
https://api.telegram.org/bot729185341:AAF0mxQmuiVr3BOtuqASy_0i870tobyq_pM/getupdates

{"ok":true,"result":[{"update_id":86206799,
"message":{"message_id":1,"from":{"id":595511839,"is_bot":false,"first_name":"DaveNISC","last_name":"www.davenisc.com\u2665\u2728\u2729","username":"DaveNISC"},"chat":
{"id":-398228019,"title":"Mikrotik","type":"group","all_members_are_administrators":true,"date":1550945488,"group_chat_created":true}}]}
```

Crear Bot con Telegram

- 1. Token: 729185341:AAF0mxQmuiVr3BOtuqASy_oi87otobyq_pM
- 2. ID de grupo: -398228019
- 3. "https://api.telegram.org/bot729185341:AAF0mxQmuiVr3BOtuqASy_oi87otobyq_pM/sendMessage?chat_id=-398228019&text=Time: [Time]; Device: [Device.FirstAddress]; Status: [Service.Status]"

Notificaciones con Telegram

The screenshot shows the Mikrotik WinBox interface for Firewall and Bandwidth Control. The main window displays a list of notifications, with 'Notification-Telegram' selected. A dialog box titled 'Notification-Telegram - Notification' is open, showing the configuration for this notification.

Notification List:

Name	Type	Notes
beep	beep	
Notification-Telegram	execute on server	
flash	flash	
log to syslog	log	
log to events	log	
popup	popup	

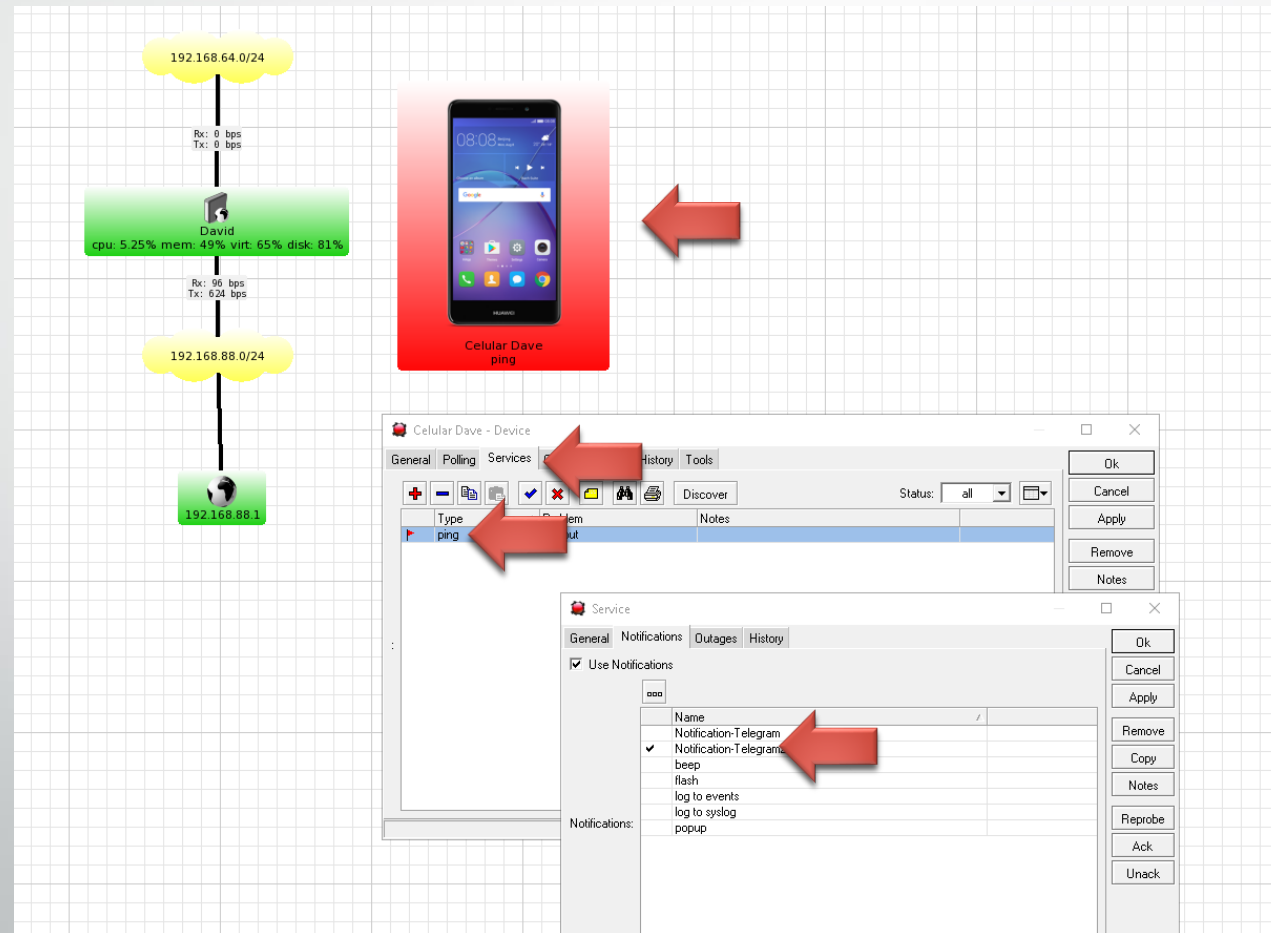
Notification Configuration Dialog:

- Name: Notification-Telegram
- Enabled:
- Type: execute on server
- Command:

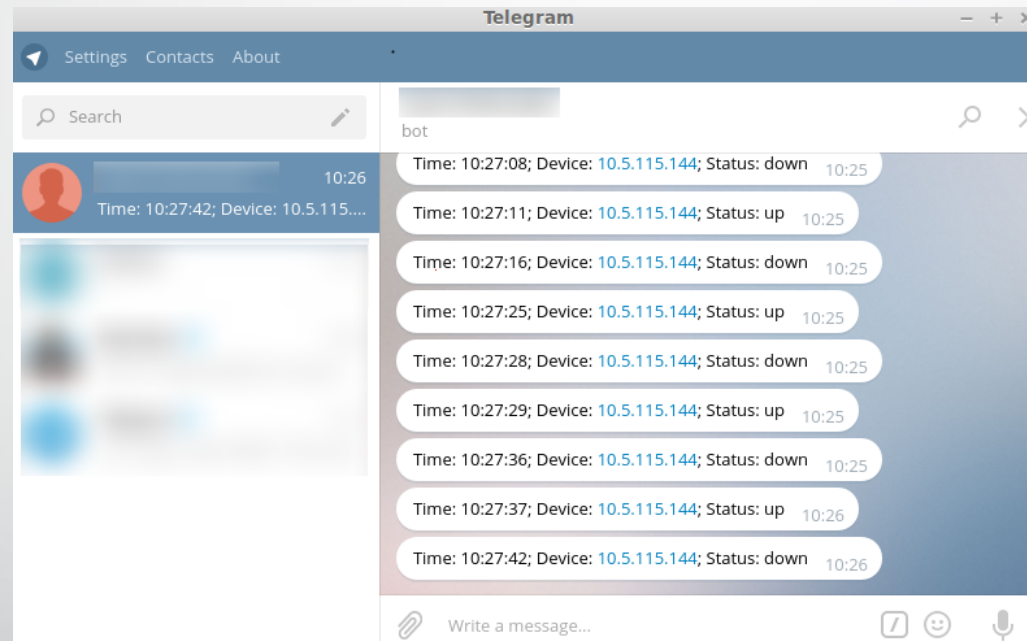
```
/tool fetch
url="https://api.telegram.org/bot309683994:AAFh8645FeAOgUbcOgUVIhtc1bmzpwI
XpA/sendMessage?chat_id=312605050&text=Time: [Time]; Device:
[Device.FirstAddress]; Status: [Service.Status]"
```

Client: rx 1.34 kbps / tx 353 bps Server: rx 0 bp

Aplicar notificación a cada host



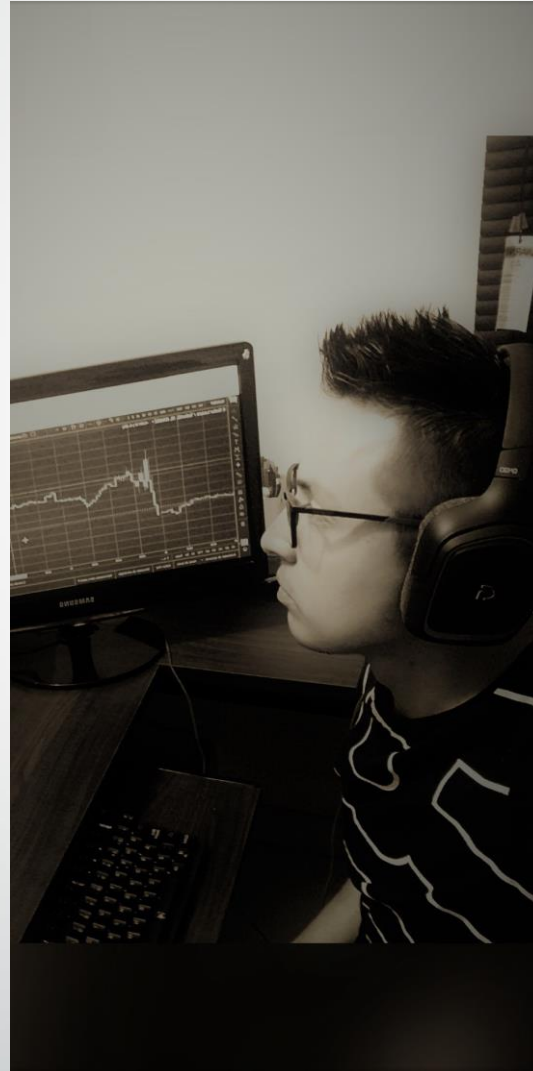
Notificaciones con Telegram



Referencias

- * https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6/Dude_Telegram_Example
- * <https://core.telegram.org/api>
- * <https://core.telegram.org/bots/api>
- * https://wiki.mikrotik.com/wiki/Manual:The_Dude_v6
- * <https://mikrotik.com/download>
- * <https://mikrotik.com/thedude>
- * <https://mikrotik.com/>

Gracias!



DaveNISC
Expertos en seguridad informática

@DaveNISC

- www.davenisc.com
- info@davenisc.com

