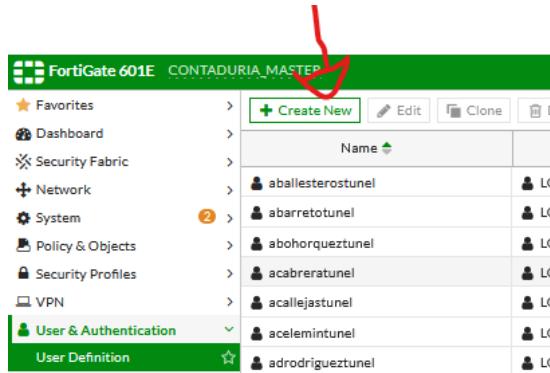


INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	1 de 10

CREACION USUARIO ACCESO VPN

1. User & Authentication

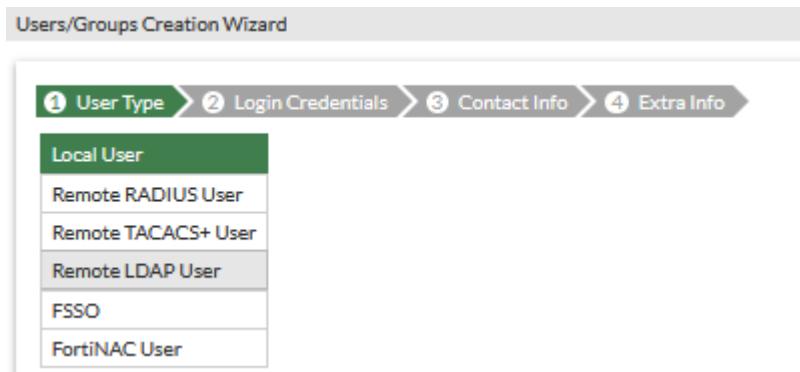


FortiGate 601E - CONTADURIA_MASTER

- Favorites
- Dashboard
- Security Fabric
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Authentication
- User Definition

Name	LC
aballesterostunel	LC
abarretotunel	LC
abohorqueztunel	LC
acaberatunel	LC
acallejastunel	LC
acelemintunel	LC
adrodrigueztunel	LC

Ingresar en **Create New** y selecciones **Remote LDAP User**.



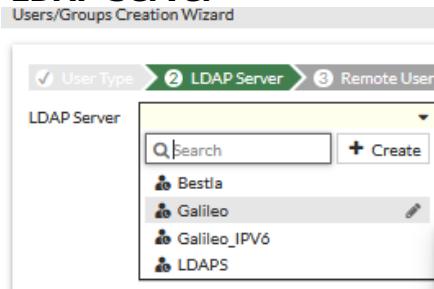
Users/Groups Creation Wizard

① User Type > ② Login Credentials > ③ Contact Info > ④ Extra Info

- Local User
- Remote RADIUS User
- Remote TACACS+ User
- Remote LDAP User**
- FSSO
- FortiNAC User

Click en Next

1.1 Seleccione Galileo en LDAP Server



Users/Groups Creation Wizard

① User Type > ② LDAP Server > ③ Remote Users

LDAP Server

Search: Galileo

- Bestia
- Galileo**
- Galileo_IPv6
- LDAPS

INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	2 de 10

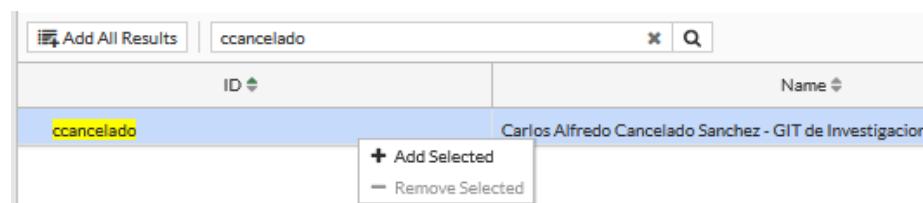
Click en Next

1.2 Escriba el nombre del usuario y de click en **Buscar (Lupa)**



The screenshot shows a search interface for 'Remote Users'. The search bar contains 'ccancelado'. A red arrow points to the search icon (magnifying glass). The results table has columns for 'ID' and 'Name'. One result is highlighted: 'ccancelado' (Carlos Alfredo Cancelado Sanchez - GIT de Investigacion y Normas).

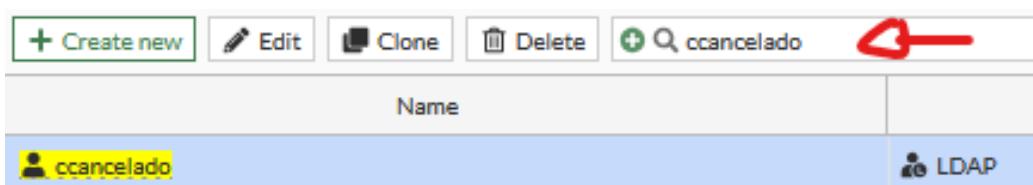
Seleccione el usuario y de click Derecho en el Mouse y selección **Add Selected**



The screenshot shows a modal dialog with a list of users. 'ccancelado' is selected and highlighted with a yellow background. Below the list are buttons for '+ Add Selected' and '- Remove Selected'. A red arrow points to the '+ Add Selected' button.

Y de click en **Submit**.

2. En **Search** ingrese el nombre del usuario y de Enter

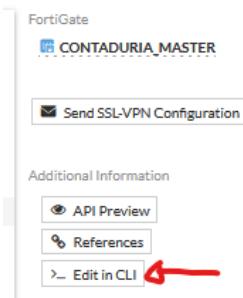


The screenshot shows a search interface with a search bar containing 'ccancelado'. A red arrow points to the search icon (magnifying glass). The results table has columns for 'Name' and 'LDAP'. One result is highlighted: 'ccancelado' (LDAP).

Seleccione el usuario y de click en **Edit**

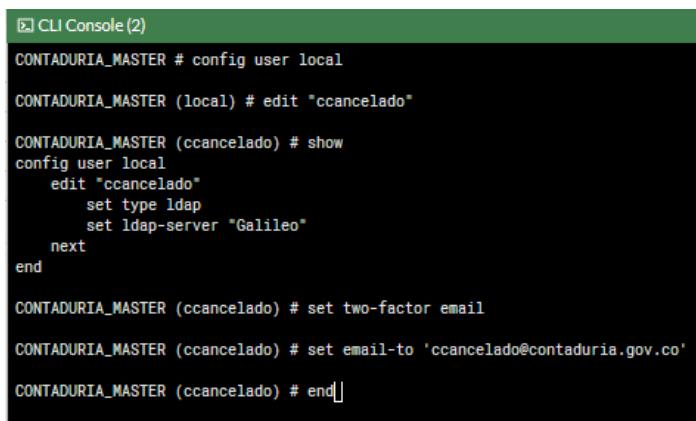
2.1. En **Additional Information** de click en **Edit in CLI**

INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	3 de 10



2.2. Escriba en su orden los siguientes comandos: en cada uno finalice con Enter

```
set two-factor email
set email-to 'correo-institucional-usuario'
end
```

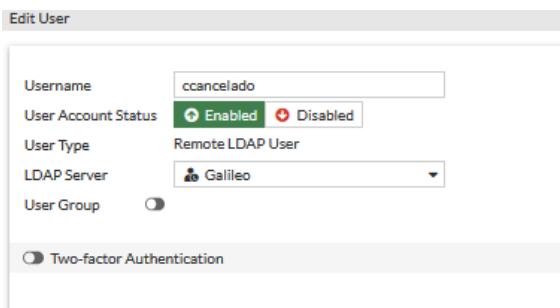


```
CLI Console (2)
CONTADURIA_MASTER # config user local
CONTADURIA_MASTER (local) # edit "ccancelado"
CONTADURIA_MASTER (ccancelado) # show
config user local
    edit "ccancelado"
        set type ldap
        set ldap-server "Galileo"
    next
end

CONTADURIA_MASTER (ccancelado) # set two-factor email
CONTADURIA_MASTER (ccancelado) # set email-to 'ccancelado@contaduria.gov.co'
CONTADURIA_MASTER (ccancelado) # end]
```

Cierre la ventana de CLI.

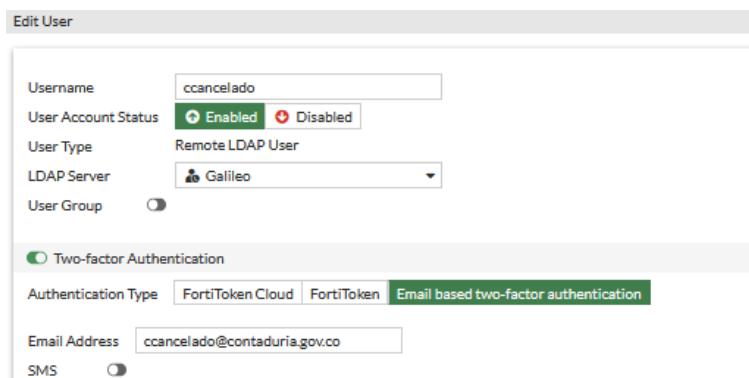
2.3. De click en OK



Username	ccancelado
User Account Status	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
User Type	Remote LDAP User
LDAP Server	Galileo
User Group	(empty)
<input type="radio"/> Two-factor Authentication	

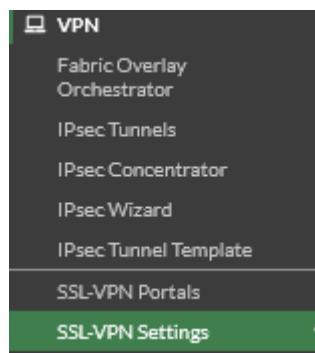
INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	4 de 10

Si realiza la búsqueda nuevamente del usuario y edita la información le debe aparecer de esta forma:

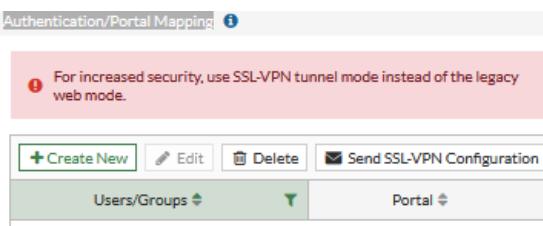


The screenshot shows the 'Edit User' form. The 'Username' field contains 'ccancelado'. The 'User Account Status' section has a green 'Enabled' button and a red 'Disabled' button. The 'User Type' is 'Remote LDAP User'. The 'LDAP Server' dropdown is set to 'Galileo'. The 'User Group' section shows a radio button. The 'Two-factor Authentication' section has a radio button and three tabs: 'FortiToken Cloud' (selected), 'FortiToken', and 'Email based two-factor authentication'. Below these are fields for 'Email Address' (ccancelado@contaduria.gov.co) and 'SMS'.

3. En el menú seleccione **VPN** y seleccione **SSL-VPN Settings**



3.1 En **Authentication/Portal Mapping** de Click en Create New

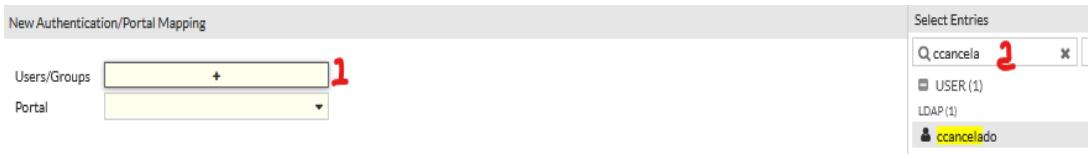


The screenshot shows the 'Authentication/Portal Mapping' interface. A red warning box says: 'For increased security, use SSL-VPN tunnel mode instead of the legacy web mode.' Below it is a toolbar with 'Create New', 'Edit', 'Delete', and 'Send SSL-VPN Configuration' buttons. There are dropdown menus for 'Users/Groups' and 'Portal'.

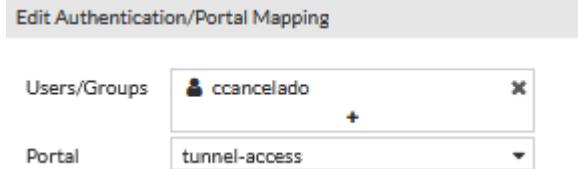
INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	5 de 10

3.2 De click en **Users/Groups (1)** y busque el nombre del usuario, de click sobre el nombre del usuario (2).

En Portal seleccione **Tunnel Access**.



De click en **OK**



De click en **Apply**

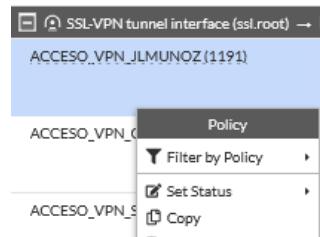
CREACION DE LAS POLÍTICAS VPN

4. En el menú seleccione **Policy & Objects** Seleccione **Firewall Policy**

4.1. Si es para conexión a **RDP (Escritorio Remoto)**, busque la siguiente sección:

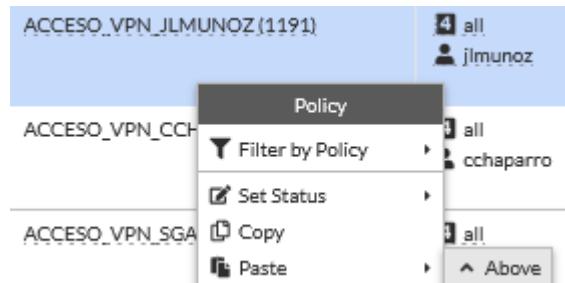


4.2. Seleccione la Primera política, de click Derecho y click en **Copy**



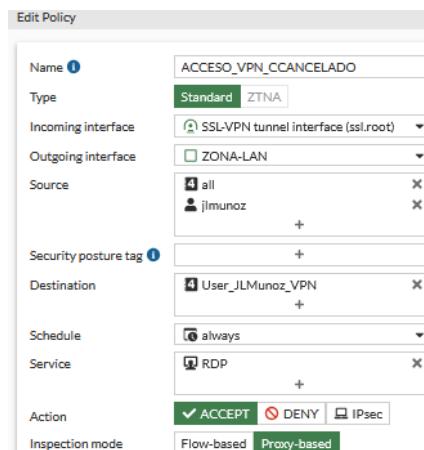
INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	6 de 10

Sobre esa misma política de click derecho y click en Paste/Above

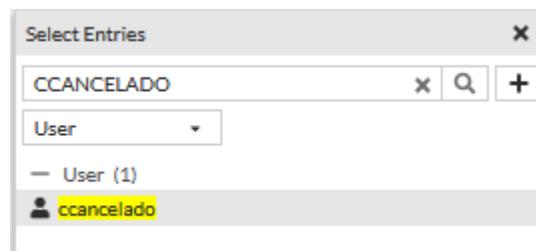


4.3. De doble click sobre la política pegada

De click en la sección de Source



En **Search** escriba el nombre del usuario y Seleccione **User**



INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	7 de 10

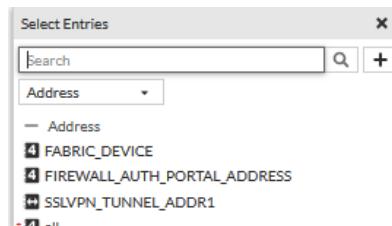
De click sobre el usuario y le debe aparecer agregado en **Source**



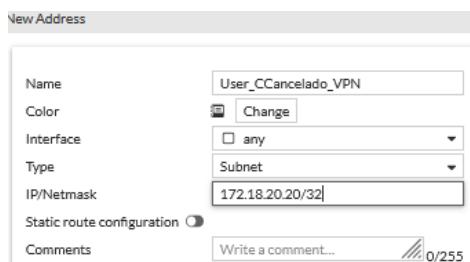
Elimine el usuario adicional dando click sobre la **X**

4.4. De click en la sección **Destination**

De click en el signo **+** y Selecciones **Address**



Cree el nuevo Objeto de Usuario ingresando el Nombre y la dirección **IP/Netmask** del equipo de oficina asignado.



De click en **OK** y en **OK**

Elimine el usuario adicional dando click en la **X**

INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	8 de 10

Security posture tag 

Destination	 User_JLMunoz_VPN   User_CCancelado_VPN  
Schedule	 always 
Service	 RDP  

Y al final todo debe quedar así:

Edit Policy

Name 	ACCESO_VPN_CCANCELADO
Type	Standard 
Incoming interface	 SSL-VPN tunnel interface (ssl.root) 
Outgoing interface	 ZONA-LAN 
Source	 all   ccancelado  
Security posture tag 	
Destination	 User_CCancelado_VPN  
Schedule	 always 
Service	 RDP  
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> IPsec
Inspection mode	<input type="radio"/> Flow-based <input checked="" type="radio"/> Proxy-based

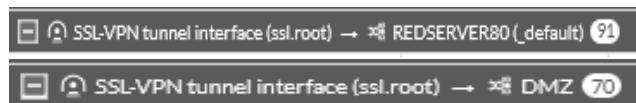
4.5. Habilite la política (Enable this Policy) y de click en OK

Enable this policy 

OK

INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	9 de 10

5. Si es conexión a VPN Directa entonces se deben crear las políticas sobre las secciones de REDSERVER80 Y DMZ



Siga los mismos pasos indicados en los ítems 4.2 y 4.3

Al final debe quedar algo así:

En el nombre de la política finalícelo con R80 para este caso.

Para la sección de Destination déjelos tal cual sin hacer ningún cambio al menos que se necesite agregar un puerto o protocolo si lo requiere para acceder a alguna aplicación.

Habilite la política y de **OK**.

INSTRUCTIVO CREACIÓN USUARIO VPN Y POLÍTICAS			
PROCESO:	GESTIÓN TICS		
PROCEDIMIENTO:	MESA DE SERVICIO		
FECHA DE APROBACIÓN:	CÓDIGO:	VERSIÓN:	PÁGINA:
24/09/2025	GTI05-INS04	1.0	10 de 10

Enable this policy 

OK

6. Creación de la política de VPN Directa sobre la DMZ.

Edit Policy

Name 	ACCESO_VPN_CCANCELADO_DMZ
Type	Standard ZTNA
Incoming interface	SSL-VPN tunnel interface (ssl.root)
Outgoing interface	DMZ
Source	<input type="checkbox"/> all <input checked="" type="checkbox"/> ccancelado
Security posture tag 	+ 
Destination	<input type="checkbox"/> Red_DMZ
Schedule	always
Service	<input type="checkbox"/> Navegacion
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> IPsec
Inspection mode	Flow-based <input checked="" type="checkbox"/> Proxy-based

Firewall/Network Options

NAT 

Enable this policy 

OK

7. Enviar el correo electrónico al usuario con el instructivo de VPN y el de Pathfinder sobre VPN.