



1. Pfsense - actif

Installation de Pfsense

Etape 1 : Créer la VM, avec les configurations ci-dessous.

Nom	ID	OS	Mémoire	RAM	CPU	Réseau	Services/Remarques
PfSense - actif	MV200	Pfsense 2.7.2	20Go	1Go	1 processor 1 cœurs	VMBR0 VMBR1 VMBR2	Em0 : 10.113.0.81/16 Em1 : 192.168.16.254/24 Em2 : 192.168.17.254/24

Configuration réseau

Etape 2 : Configurer les interfaces dans pfsense, via la console et attribuer leurs passerelles.

Em0 : DHCPv4

Em1 : 192.168.16.254/24

Em2 : 192.168.17.254/24

```
WAN (wan)      -> vtnet0      -> v4/DHCP4: 10.113.113.26/16
IT (lan)       -> vtnet1      -> v4: 192.168.16.254/24
SRV (opt1)    -> vtnet2      -> v4: 192.168.17.254/24
```

Ubuntu - client

Installation de Ubuntu

Nom	ID	OS	Mémoire	RAM	CPU	Réseau	@IP
Ubuntu-client	MV120	Ubuntu 24.04	32Go	2Go	1 processor 1 cœurs	VMBR1	Attribué via DHCP

Interface graphique Pfsense

Accéder à l'interface graphique de Pfsense avec : <http://192.168.17.254/>

Modifier le nom des interfaces :

Em0 : WAN

Em1 : IT

Em2 : SRV

Activation des logs sur les interfaces

Créer des règles en autorisant tout et activer les logs.



Floating WAN IT SRV OPT2 OPT3

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/891 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

↑ Add ↓ Add 🗑️ Delete ⏸️ Toggle 📄 Copy 💾 Save ➕ Separator

Configuration du portail captif – Gestion d'utilisateurs

PfSense dispose d'un portail captif. Le portail captif force les clients d'un réseau à afficher une page Web d'authentification avant de pouvoir se connecter à Internet.

Il est utilisé dans des réseaux qui assurent un accès public tels que les espaces d'accueil, établissements scolaires.

Important : Ne pas modifier le langage de l'interface en Français avant la configuration du portail car il y a un Bug lors de la sauvegarde des modifications dans certaines versions.

En revanche, une fois la configuration terminée et validée, vous pouvez modifier la langue de l'interface en Français.

Services > Captive Portal

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾

Status / Dashboard

Auto Config Backup

Captive Portal

Cliquer sur « + Add »

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / Captive Portal

Captive Portal Zones

Zone	Interfaces	Number of users	Description	Actions
------	------------	-----------------	-------------	---------

+ Add

Renseigner le Nom du portail captif et sa description.



Services / Captive Portal / Add Zone

Add Captive Portal Zone

Zone name PORTAIL
Zone name. Can only contain letters, digits, and underscores (_) and may not start with a digit.

Zone description Portail Captif
A description may be entered here for administrative reference (not parsed).

Save & Continue

- Activer « **Enable Captive Portal** ».
- Sélectionner l'interface « I T ».
- Maximum concurrent connections : **1** (Limite le nombre de connexions simultanées d'un même utilisateur).
- Idle timeout (Minutes) : Choisir entre **1 à 5** (Les clients seront déconnectés après cette période d'inactivité).

Services / Captive Portal / PORTAIL / Configuration

Configuration MACs Allowed IP Addresses Allowed Hostnames Vouchers High Availability File Manager

Captive Portal Configuration

Enable ☒ Enable Captive Portal

Description portail captif
A description may be entered here for administrative reference (not parsed).

Interfaces WAN IT SRV OPT2
Select the interface(s) to enable for captive portal.

Maximum concurrent connections 1
Limits the number of concurrent connections to the captive portal HTTP(S) server. This does not set how many users can be logged in to the captive portal, but rather how many connections a single IP can establish to the portal web server.

Idle timeout (Minutes) 5
Clients will be disconnected after this amount of inactivity. They may log in again immediately, though. Leave this field blank for no idle timeout.

- Activer « **Enable logout popup window** » (une fenêtre popup permet aux clients de se déconnecter).
- Définir « **Pre-authentication Redirect URL** » (**URL HTTP** de redirection par défaut. Les visiteurs ne seront redirigés vers cette URL après authentification que si le portail captif ne sait pas où les rediriger).
- Définir « **After authentication Redirection URL** » (**URL HTTP** de redirection forcée. Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont initialement tenté d'accéder après s'être authentifiés).
- Activer « **Disable Concurrent user logins** » (seule la connexion la plus récente par nom d'utilisateur sera active).
- Activer « **Disable MAC filtering** » (nécessaire lorsque l'adresse MAC du client ne peut pas être déterminée).



Logout popup window	<input checked="" type="checkbox"/> Enable logout popup window If enabled, a popup window will appear when clients are allowed through the captive portal. This allows clients to explicitly disconnect themselves before the idle or hard timeout occurs.
Pre-authentication redirect URL	<input type="text" value="http://www.google.fr/"/> Set a default redirection URL. Visitors will be redirected to this URL after authentication only if the captive portal doesn't know where to redirect them. This field will be accessible through \$PORTAL_REDIRECTURL\$ variable in captiveportal's HTML pages.
After authentication Redirection URL	<input type="text" value="http://www.google.fr"/> Set a forced redirection URL. Clients will be redirected to this URL instead of the one they initially tried to access after they've authenticated.
Blocked MAC address redirect URL	<input type="text"/> Blocked MAC addresses will be redirected to this URL when attempting access.
Concurrent user logins	<input checked="" type="checkbox"/> Disable Concurrent user logins If enabled only the most recent login per username will be active. Subsequent logins will cause machines previously logged in with the same username to be disconnected.
MAC filtering	<input checked="" type="checkbox"/> Disable MAC filtering If enabled no attempts will be made to ensure that the MAC address of clients stays the same while they are logged in. This is required when the MAC address of the client cannot be determined (usually because there are routers between pfSense and the clients). If this is enabled, RADIUS MAC authentication cannot be used.

- Sélectionner « **Use an Authentication backend** ».
- Sélectionner « **Local Database** » pour « Authentication Server ».
- **Attention** : Ne pas sélectionner « Local Database » pour « Secondary Authentication Server ».
- Activer « **Local Authentication Privileges** » (Autoriser uniquement les utilisateurs avec les droits de « Connexion au portail captif »).

Puis cliquer « Save »

Authentication	
Authentication Method	<div>Use an Authentication backend</div> <div>Select an Authentication Method to use for this zone. One method must be selected. - "Authentication backend" will force the login page to be displayed and will authenticate users using their login and password, or using vouchers. - "None" method will force the login page to be displayed but will accept any visitor that clicks the "submit" button. - "RADIUS MAC Authentication" method will try to authenticate devices automatically with their MAC address without displaying any login page.</div>
Authentication Server	<div>Local Database</div> <div>You can add a remote authentication server in the User Manager. Vouchers could also be used, please go to the Vouchers Page to enable them.</div>
Secondary authentication Server	<div>Local Database</div> <div>You can optionally select a second set of servers to authenticate users. Users will then be able to login using separated HTML inputs. This setting is useful if you want to provide multiple authentication method to your users. If you don't need multiple authentication method, then leave this setting empty.</div>
Reauthenticate Users	<div><input type="checkbox"/> Reauthenticate connected users every minute</div> <div>If reauthentication is enabled, request are made to the server for each user that is logged in every minute. If an access denied is received for a user, that user is disconnected from the captive portal immediately. Reauthentication requires user credentials to be cached in the captive portal database while a user is logged in; The cached credentials are necessary for the portal to perform automatic reauthentication requests.</div>
Local Authentication Privileges	<div><input checked="" type="checkbox"/> Allow only users/groups with "Captive portal login" privilege set</div>
HTTPS Options	
Login	<div><input type="checkbox"/> Enable HTTPS login</div> <div>When enabled, the username and password will be transmitted over an HTTPS connection to protect against eavesdroppers. A server name and certificate must also be specified below.</div>
<div>Save</div>	



Résultat

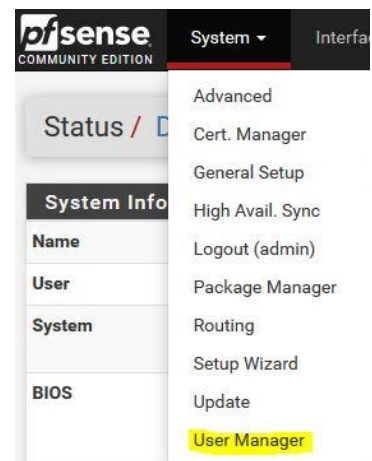
Services / Captive Portal				
Captive Portal Zones				
Zone	Interfaces	Number of users	Description	Actions
PORTAIL	IT	0	portail captif	

Configuration du Groupe et des Utilisateurs pour la délégation du Portail Captif

Création d'un groupe et utilisateur qui aura pour fonction de créer des Utilisateurs autorisés à se connecter au Portail Captif. Ce groupe et utilisateurs associés auront seulement le droit de créer des Utilisateurs du Portail Captif.

Sélectionner : System – User Manager

Onglet 'Groups », cliquer sur « + Add »



System / User Manager / Groups			
Users	Groups	Settings	Authentication Servers
Groups			
Group name	Description	Member Count	Actions
all	All Users	1	
admins	System Administrators	1	

Renseigner le Nom du groupe « Utilisateurs »



System / User Manager / Groups / Edit

Users Groups Settings Authentication Servers

Group Properties

Group name Utilisateurs

Scope Local
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description
Group description, for administrative information only

Group membership
admin

Not members Members

» Move to "Members" « Move to "Not members"








Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Dans le menu « Actions », modifier le groupe créé en cliquant sur le stylo

System / User Manager / Groups

Users Groups Settings Authentication Servers

Groups

Group name	Description	Member Count	Actions
Utilisateurs		0	  
admins	System Administrators	1	 
all	All Users	1	 

+ Add

Cliquez sur « + Add » rubrique « **Assigned Privileges** ».

Group Properties

Group name Agent

Scope Local
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description Delegation Creation Utilisateurs Portail
Group description, for administrative information only

Group membership
admin

Not members Members

» Move to "Members" « Move to "Not members"

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Assigned Privileges

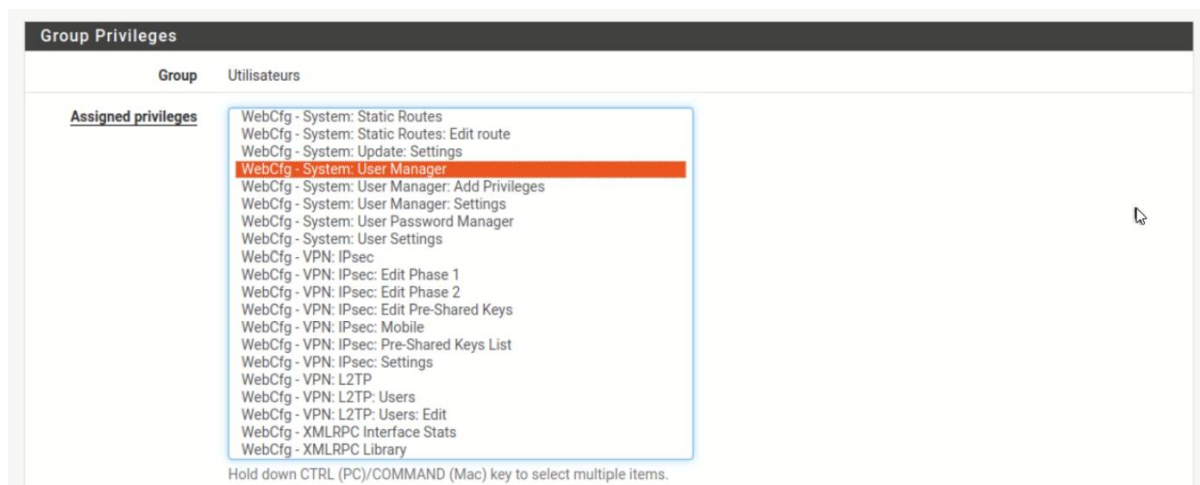
Name	Description	Action
------	-------------	--------

+ Add



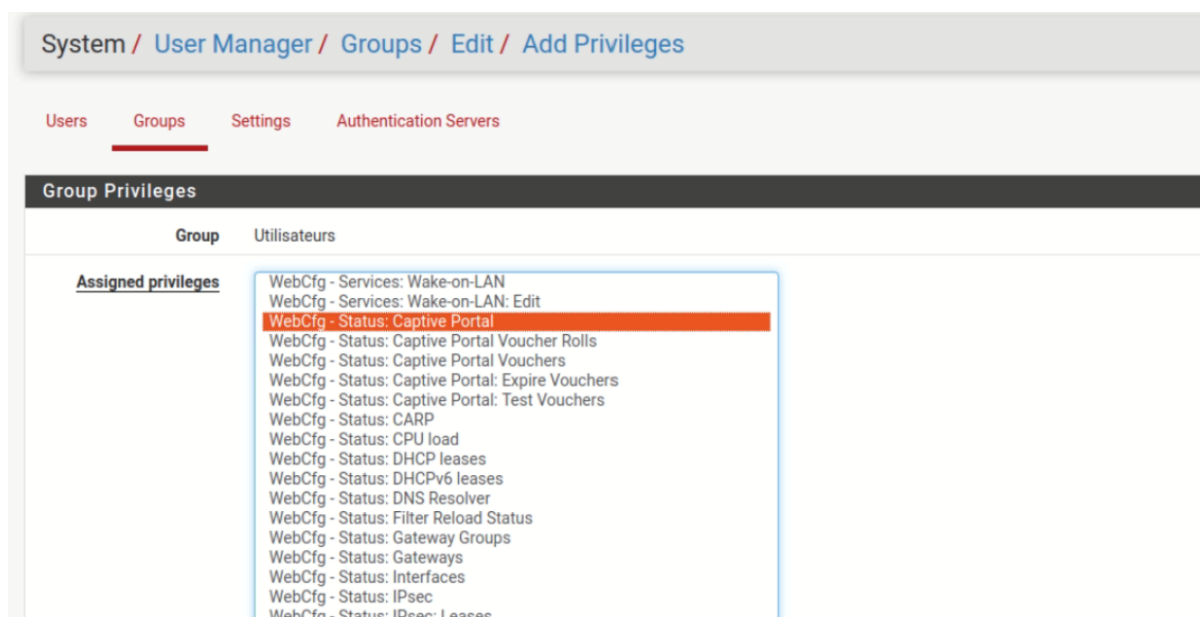
Sélectionnez dans la liste « **WebCf – System: User Manager** » (Accès à la page de gestion des utilisateurs « User Manager »)

Puis cliquez sur « **Save** »



Revenir à la rubrique « **Assigned Privileges** » en cliquant sur « **+ Add** »

Sélectionnez dans la liste « **WebCf – Status: Captive Portal** » (Voir le Status des utilisateurs connectés »)



Puis cliquez sur « **Save** »

Vérifier les droits, puis cliquez sur « **Save** »



Assigned Privileges

Name	Description	Action
WebCfg - System: User Manager	Allow access to the 'System: User Manager' page. (admin privilege)	
WebCfg - Status: Captive Portal	Allow access to the 'Status: Captive Portal' page.	
Security notice: Users in this group effectively have administrator-level access		

Save Add

Création des Utilisateurs

Onglet « **Users** », cliquez sur « **+ Add** »

System / User Manager / Users

Users Groups Settings Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	

Add Delete

Entrer un **Nom d'utilisateur** « osissoko », son **mot de passe** et sa **description** (Agent autorisé à créer des utilisateurs du Portail Captif).

Sélectionner dans « **Group membership** » le groupe « Agents » précédemment créé. Cliquez sur « **Move to Member of list** » puis « **Save** »

User Properties

Defined by USER

Disabled ☐ This user cannot login

Username

Password

Full name
User's full name, for administrative information only

Expiration date
Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY

Custom Settings ☐ Use individual customized GUI options and dashboard layout for this user.

Group membership

Not member of Member of

Move to "Member of" list Move to "Not member of" list

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Certificate No private CAs found. A private CA is required to create a new user certificate. Save the user first to import an external certificate.



System / User Manager / Users

Users Groups Settings Authentication Servers

Users

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input checked="" type="checkbox"/>	osissoko	Omar SISSOKO	✓	Utilisateurs	

[+ Add](#) [Delete](#)

Configuration du groupe et des utilisateurs autorisés à se connecter au Portail Captif

Ce groupe et utilisateurs associés auront seulement le droit d'utiliser le Portail Captif.

Onglet « **Groups** », cliquez sur « **+ Add** »

System / User Manager / Groups

Users Groups Settings Authentication Servers

Groups

Group name	Description	Member Count	Actions
Utilisateurs		1	
admins	System Administrators	1	
all	All Users	2	

[+ Add](#)

Renseigner le **Nom du Groupe** « Portail – user management » et sa **description** « Utilisateurs du Portail ». Cliquez « **Save** »

Group Properties

Group name

Scope
Warning: Changing this setting may affect the local groups file, in which case a reboot may be required for the changes to take effect.

Description
Group description, for administrative information only

Group membership

Not members












Members

[Move to "Members"](#) [Move to "Not members"](#)

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Dans le menu « Actions », **modifier** le groupe créé en cliquant sur le stylo.



Users	Groups	Settings	Authentication Servers
Groups			
Group name	Description	Member Count	Actions
Portail	utilisateurs du portail captif	3	  
admins	System Administrators	2	 
all	All Users	4	 
utilisateurs	délégation création utilisateurs portail captif	3	  
			

Cliquez sur « **+ Add** » rubrique « **Assigned Privileges** » .

Group Properties

Group name

Portail

Scope

Local

Description

Group membership

admin

osissoko

Not members

Members

>> Move to 'Members'

<< Move to 'Not members'

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Sélectionnez dans la liste « **User – Services: Captive Portal login** » (Autorisé seulement a se connecter au Portail Captif)

Puis cliquez sur « **Save** »

Group Privileges

Group

Portail

Assigned privileges

System - HA node sync

User - Config: Deny Config Write

User - Notices: View

User - Notices: View and Clear

User - Services: Captive Portal login

User - System: Copy files (scp)

User - System: Copy files to home directory (chrooted scp)

User - System: Shell account access

User - System: SSH tunneling

User - VPN: IPsec xauth Dialin

User - VPN: L2TP Dialin

User - VPN: PPPOE Dialin

WebCfg - AJAX: Get Service Providers

WebCfg - AJAX: Get Stats

WebCfg - All pages

WebCfg - Crash reporter

WebCfg - Dashboard (all)

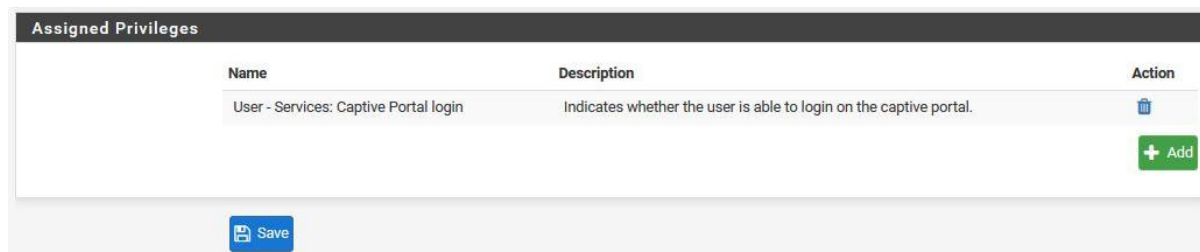
WebCfg - Dashboard widgets (direct access).

WebCfg - Diagnostics: ARP Table

WebCfg - Diagnostics: Authentication

Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.

Vérifier les droits, puis cliquez sur « **Save** »



Connexion avec le compte « osissoko »

Cet utilisateur a seulement le droit de créer des Utilisateurs du Portail Captif par délégation et de voir le Statut des utilisateurs connectés.

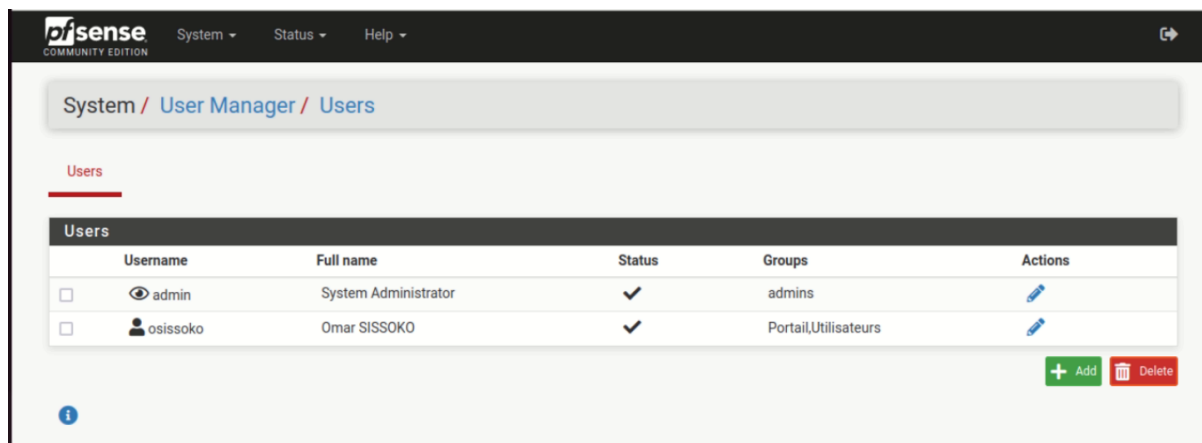
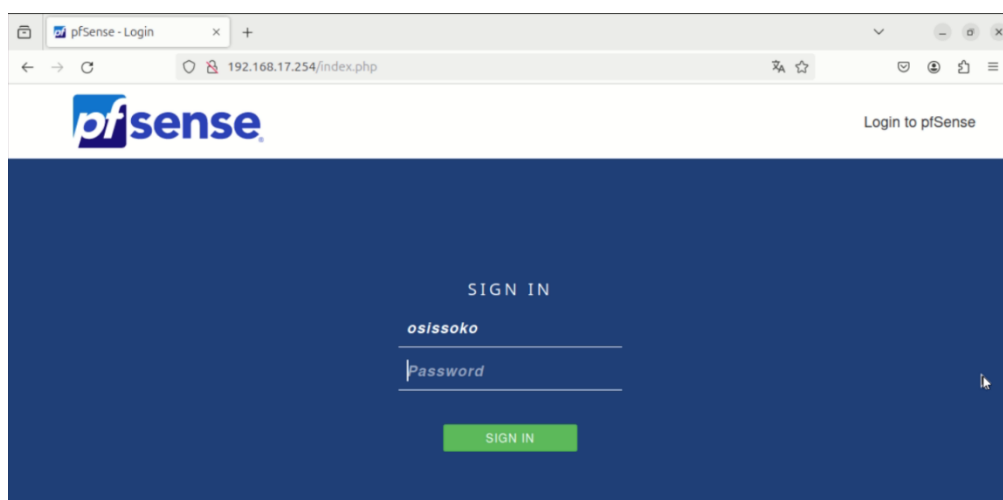


Tableau de bord restreint. Seulement les fonctions de création d'utilisateur et de Statut du Portail Captif sont disponibles.

Le « Statut du Portail Captif » permet de voir les utilisateurs connectés et de les déconnecter si besoin ...



Créer un compte depuis le compte « osissoko »

The screenshot shows the PISense User Manager interface. At the top, there's a navigation bar with 'System / User Manager / Users'. Below this, a table lists users. The 'osissoko' user is highlighted.

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	osissoko	Omar SISSOKO	✓	Portail,Utilisateurs	

At the bottom right, there are '+ Add' and 'Delete' buttons.

Cliquer sur “ + Add”

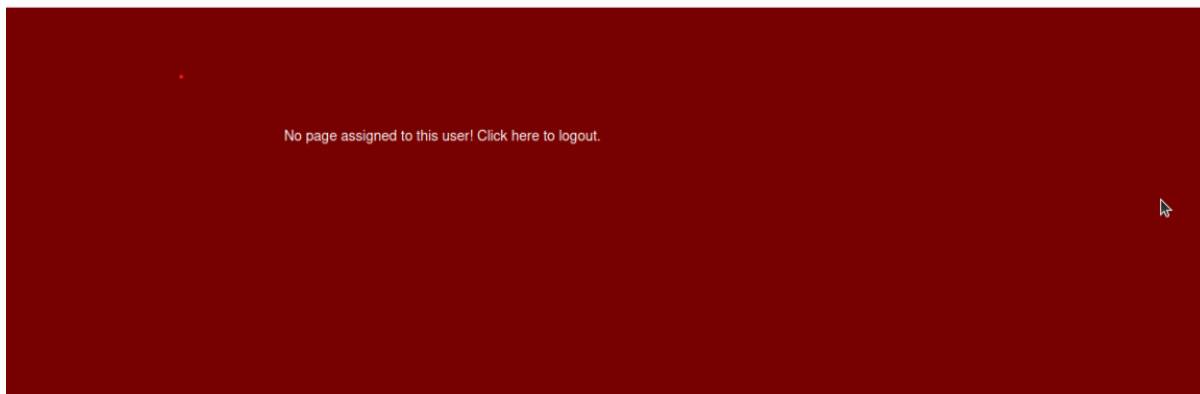
The screenshot shows the 'User Properties' form. It includes fields for Username (test), Password, Full name (TEST), Expiration date, and Group membership (Utilisateurs, admins, Portail). There are also buttons for 'Move to "Member of" list' and 'Move to "Not member of" list'.

The screenshot shows the PISense User Manager interface with the new user 'test' added to the list.

	Username	Full name	Status	Groups	Actions
<input type="checkbox"/>	admin	System Administrator	✓	admins	
<input type="checkbox"/>	osissoko	Omar SISSOKO	✓	Portail,Utilisateurs	
<input checked="" type="checkbox"/>	test	TEST	✓	Portail	

At the bottom right, there are '+ Add' and 'Delete' buttons.

Test en se connectant au compte “Test”



On a assigné aucune fonctionnalité mais la session est bien connectée.