



Guide d'installation

**XXII CORE REAL TIME
V.2.0.0**

Version guide (Genetec) - 2.0

Auteurs & historique des modifications.

Contributeurs

Auteurs	Postes
Nathan LAFONTAINE	Technical Manager
Stanislas MAHIEUX	Directeur de la formation

Historique du document

Auteurs	Date	Modifs
Nathan LAFONTAINE	5 Janvier 2023	Création du document
Stanislas MAHIEUX	17 Janvier 2023	Complémentation du document

Sommaire.

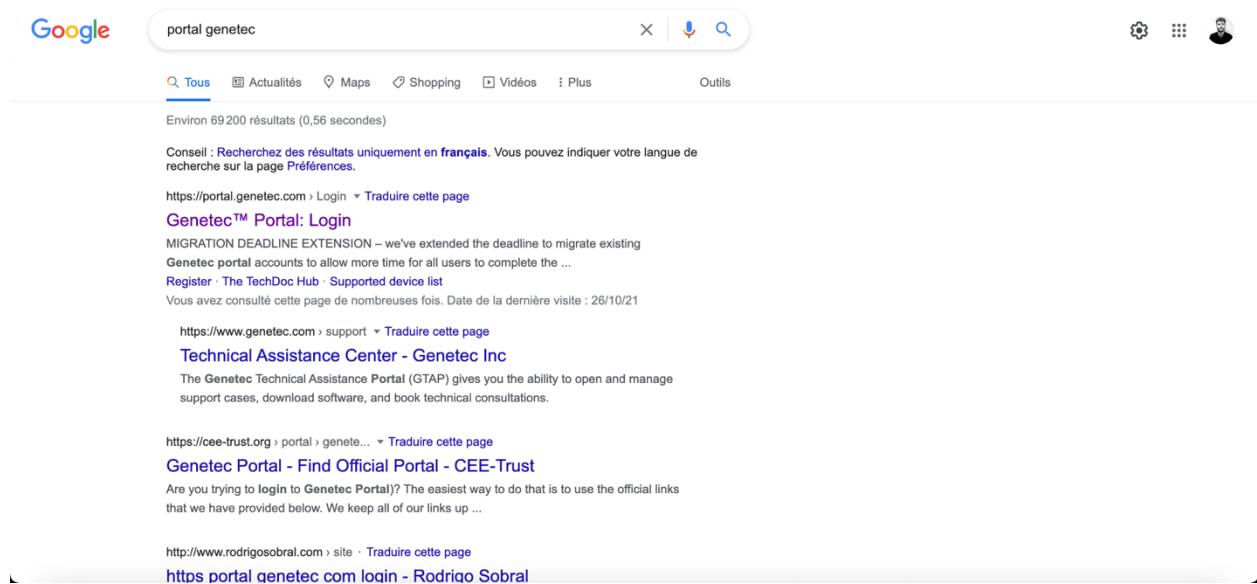
Auteurs & historique des modifications.	2
Contributeurs	2
Historique du document	2
FR_Guide de paramétrage (GENETEC) - XXII CORE REAL TIME V.2.0.0 (v1)	4
I - Préparation du Security Center	4
1 - Télécharger la licence et le “part number” XXII CORE	4
2 - Ajouter la licence avec le “part number” XXII CORE.	6
3 - Vérification des paramètres GENETEC : Création d'un utilisateur	9
5 - Vérification des paramètres GENETEC : Activer le Web SDK	14
II - Installation physique dans la baie	15
1 - Liste pré-requis avant installation : version R1 2021 du XProtect Corporate	15
2 - Étape 1 : serveur et baie de serveurs	16
3 - Étape 2 : serveur et communication	17
4 - Étapes 3 : les ingress - ajout & méthodes (Windows)	19
5 - Étape 4 : activation des licences XXII CORE	23
6 - Étape 5 : mise en action de XXII Core	24

Guide de paramétrage (GENETEC) - XXII CORE REAL TIME

I - Préparation du Security Center

1 - Télécharger la licence et le “part number” XXII CORE

- **Télécharger la licence et le “part number” XXII CORE sur le Portal Genetec**
 - **Pré-requis** : faire la demande de la nouvelle licence avant de réaliser cette étape.
 - Également, si Genetec a fourni la licence directement par mail, cette étape est inutile. Passer directement à l'étape suivante.
- **Ouvrir un navigateur et saisir “Portal Genetec”**
- **Saisir les identifiants Genetec Portal (si vous ne les possédez pas, contactez directement Genetec).**



- Cliquer sur “Technical Assistance”, puis “System Management”

The screenshot shows the Genetec Portal interface. The left sidebar has three main categories: Technical Assistance, TechDoc Hub, and Technology Partners. The 'Technical Assistance' category is highlighted with a green box. A dropdown menu for 'System Management' is open, also highlighted with a green box. The menu items include Home, Dashboard, Case Management, System Management, System Availability Monitor, Genetec™ Advantage Benefits, Product Lifecycle, Supported Devices, Training, KiwiVision Hardware Calculator, Tools, Product Download, Forum, and Contact Us. The main content area displays system information for 'SDK Package' with System ID GSC-191105-517037. It shows License status as 'Active until J...', Genetec™ Advantage coverage as 'This system h...', and End user as 'XXII'. On the right, there's a section for 'Genetec™ Advantage Information' stating 'This system is not covered by Genetec™ Advantage'.

- Sélectionner la licence concernée
- Scroller jusqu'à la section “Licence Information”.
 - Sous “Licence Key”, cliquer sur “Download”
 - La licence est à présent téléchargée.
- Le fichier doit ressembler à ça :

If a system ID is missing in this list, please contact salesadmin@genetec.com.

Results 4 of 4	
System Name	System ID
DEMO XXII	DEMO XXII LICENSE
SDK Package	SDK PACKAGE LICENSE

License information

Version: Security Center 5.8

Product: Security Center 5.8 ()

Machine	Status	Validation Key	Licenses Key
Directory	Activated	Download	Download

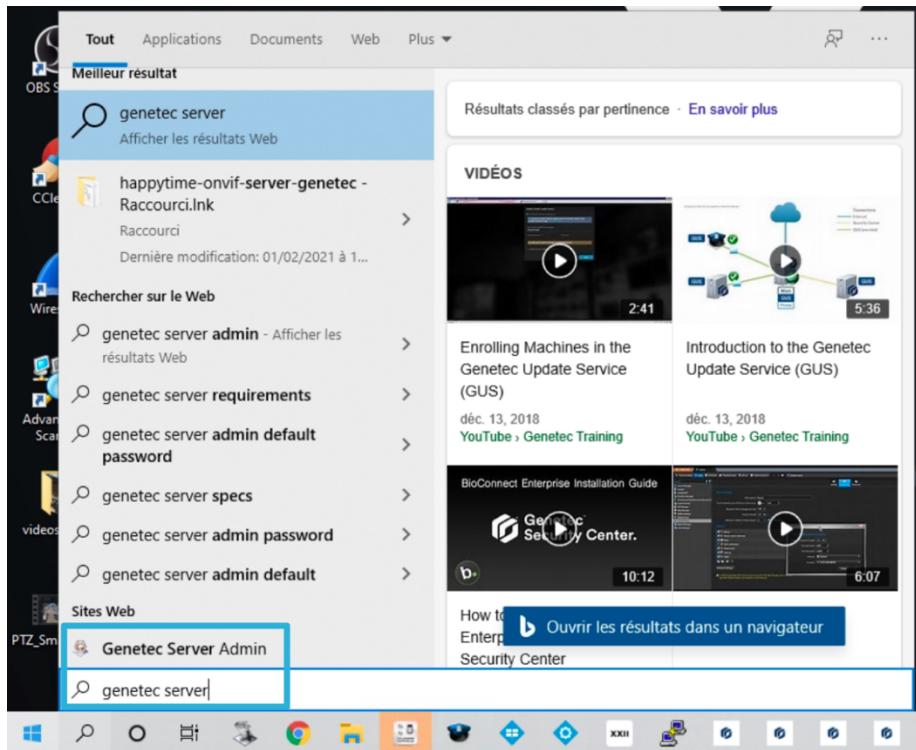
System History

Type	Description	Date
System Updated	System updated successfully. Updated fields: Expiry Date	2021/06/29
System Updated	System updated successfully. Updated fields: Expiry Date	2020/09/24
System Created	System created successfully.	2019/11/05

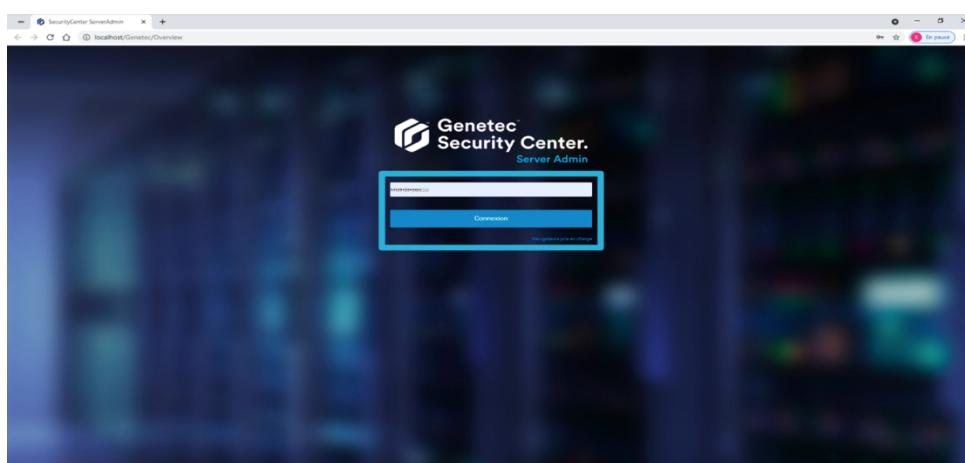


2 - Ajouter la licence avec le “part number” XXII CORE.

- **Saisir dans la recherche Windows :**
 - “genetec server” et chercher “Genetec Server Admin”.
- **Cliquer sur le fichier pour l’ouvrir**
 - Le navigateur, par défaut, va s’ouvrir avec une page “login”.



- **Si le navigateur par défaut ne s’ouvre pas, ouvrir un navigateur et saisir l’adresse suivante :**
 - localhost/Genetec/Overview
- **Saisir le mot de passe d’administration du Genetec Server Admin.**
 - **Remarque :** Ce mot de passe est paramétré lors de la première installation du Security Center



- Cliquer en haut, sur “Licence”.

Licence

Paramètres de connexion

SMTP

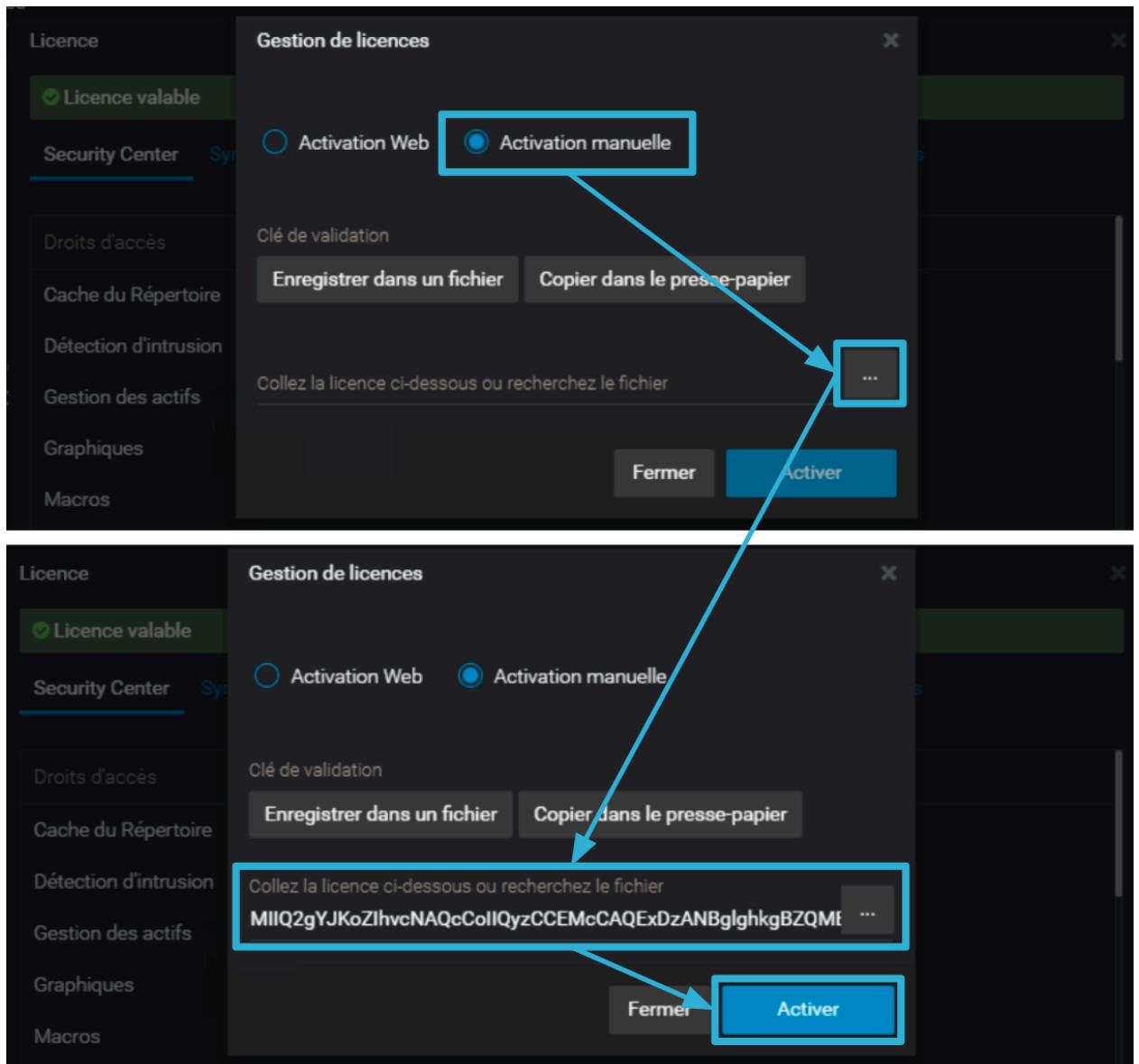
- Cliquer en haut, sur “Modifier”.

- La page de gestion de la licence s’ouvre, toutes les informations relative à votre licence Genetec Security Center sont ici.

Droits d'accès	Assistance
Cache du Répertoire	Non pris en charge
Détection d'intrusion	Non pris en charge
Gestion des actifs	Non pris en charge
Graphiques	Pris en charge
Macros	Pris en charge
Niveau de risque	Pris en charge
Nombre d'Active Directory	1

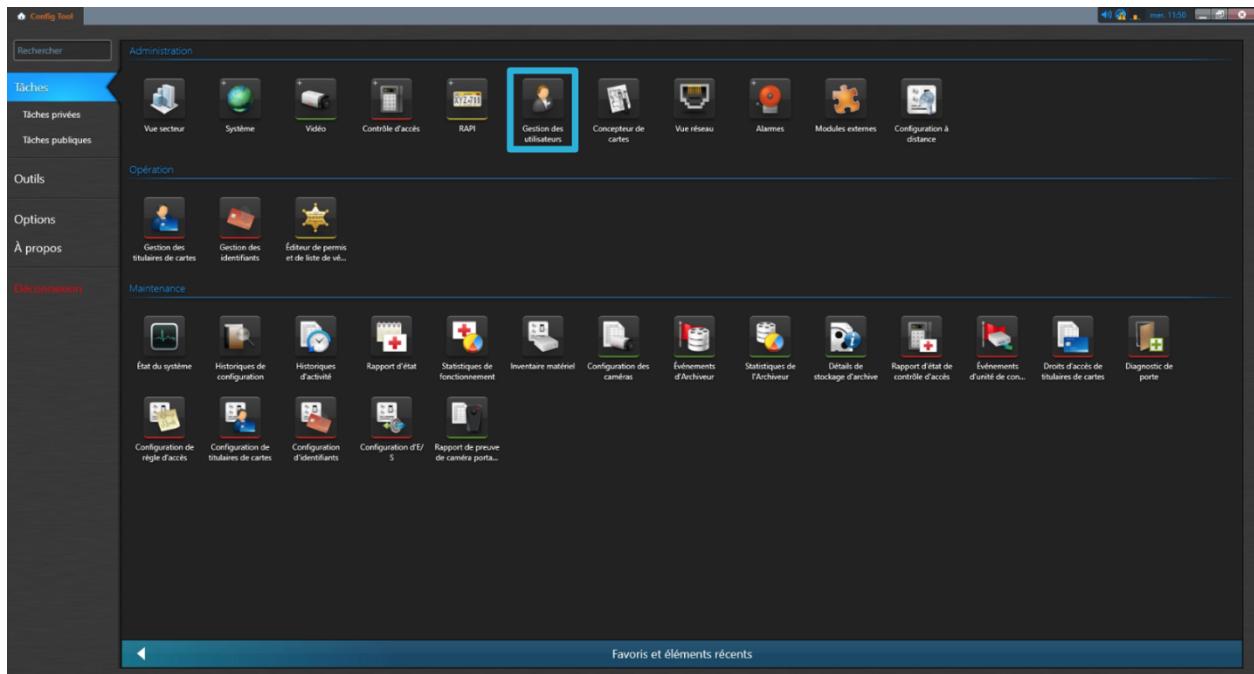
Bon de commande Modifier Fermer

- Cliquer sur “Activation manuelle” puis sur “...”
- Sélectionner le fichier de licence .lic, préalablement téléchargé depuis le Portal Genetec. Le fichier de licence est bien importé.
- Cliquer sur “Activer” pour valider l’action.
 - Félicitation, la licence est maintenant à jour.
- **Remarques** : faire attention à la date d’expiration de la licence, bien souvent c’est une licence de démo avec une date d’expiration à 30 jours. La licence perpétuelle coûte 193 € MSRP.

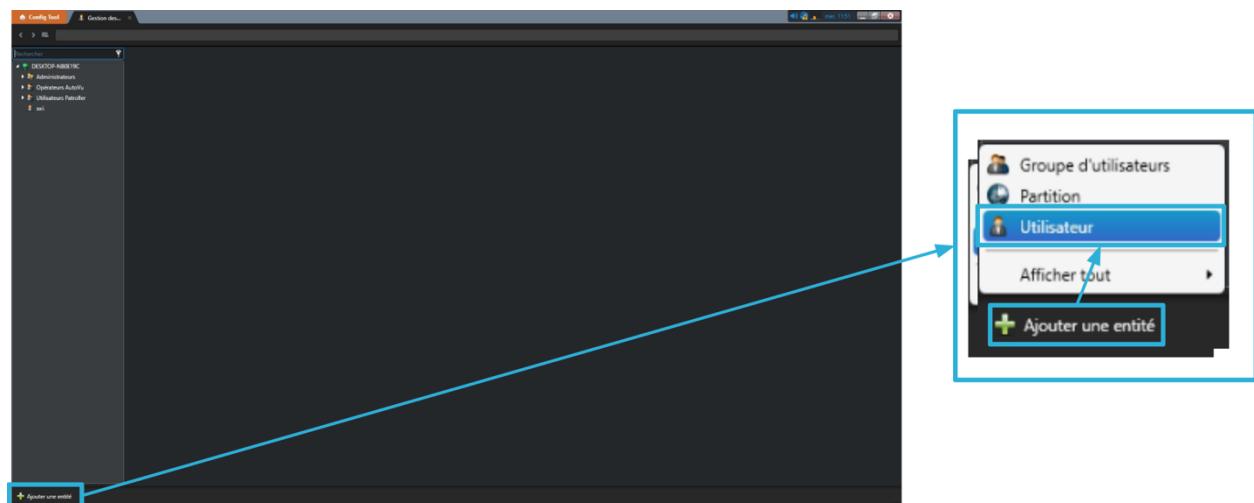


3 - Vérification des paramètres GENETEC : Création d'un utilisateur

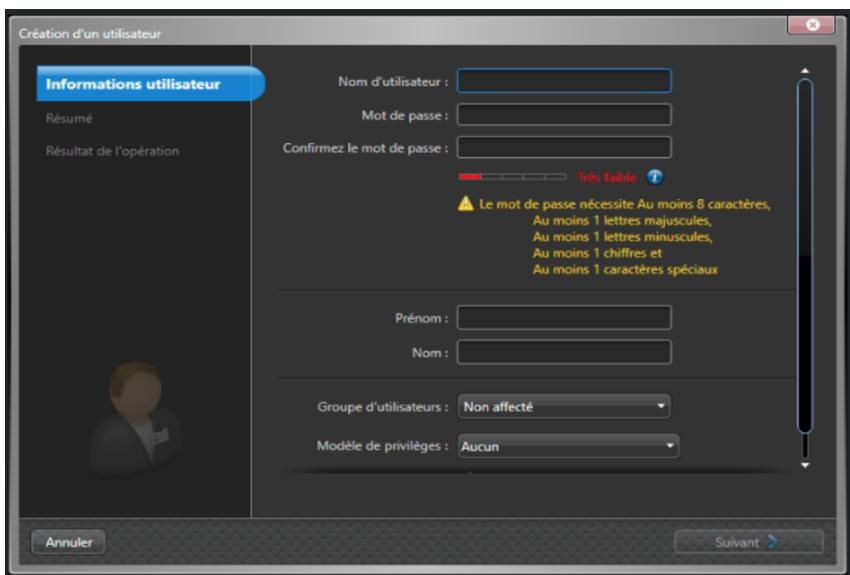
- **Rendez-vous dans le “config tool” et cliquer sur “gestion des utilisateurs”.**



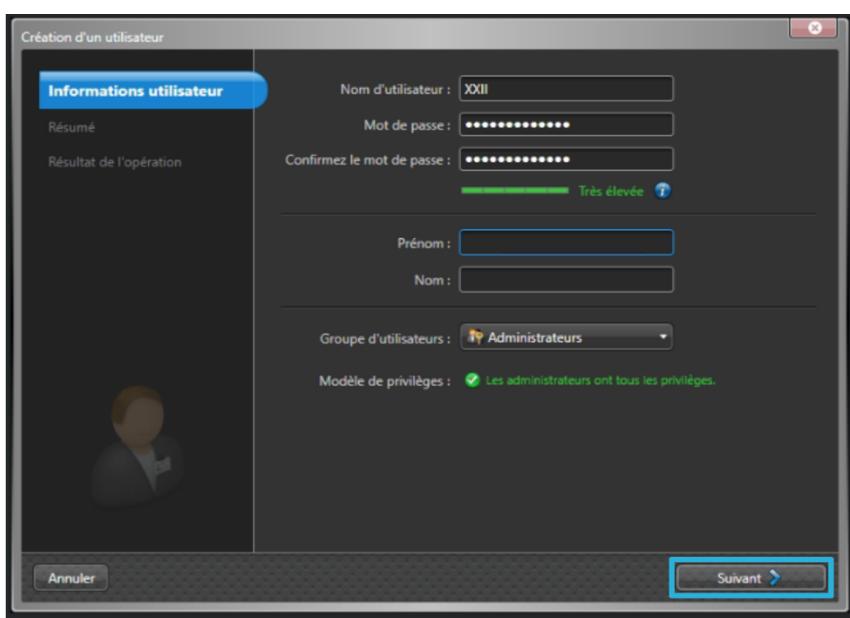
- **Cliquer sur “Ajouter une entité” et enfin cliquer sur “utilisateurs”.**



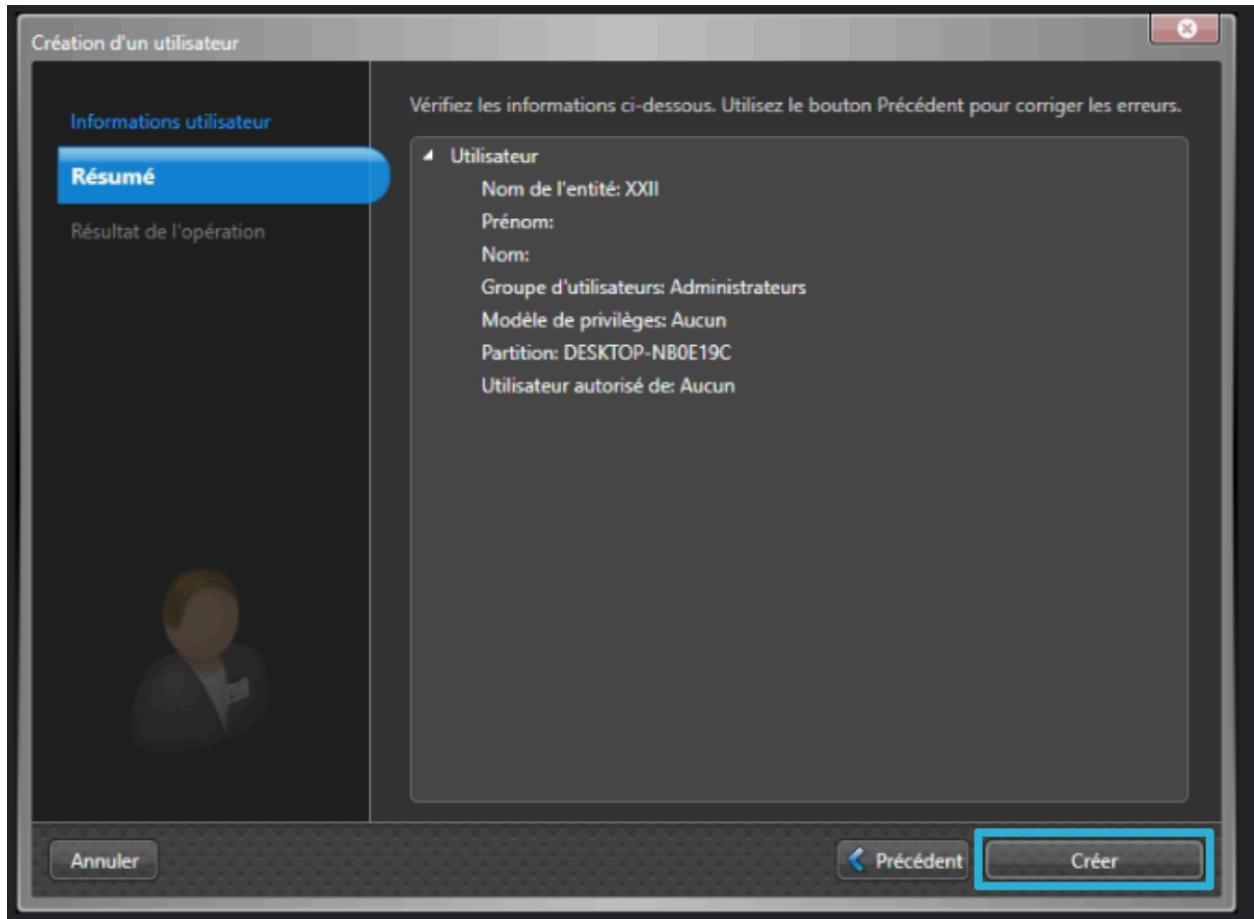
- Une fenêtre “Création d'un utilisateur” s'ouvre, saisir les informations suivantes :
 - Nom d'utilisateur : XXII
 - Mot de passe : XXIICore2020!
 - Confirmez le mot de passe : XXIICore2020!
 - Prénom : vide
 - Nom : vide
 - Groupe d'utilisateur : Administrateurs (cliquer sur administrateurs directement)
 - Modèles de priviléges : Les administrateurs ont tous les priviléges



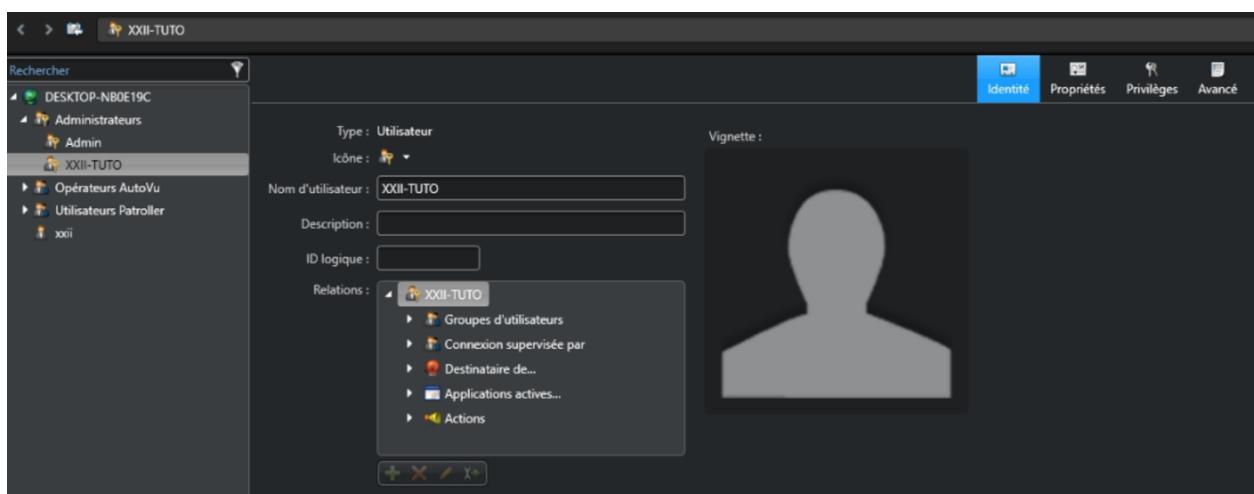
- Cliquer sur “suivant”, si votre fenêtre est similaire à l'exemple ci-dessous.



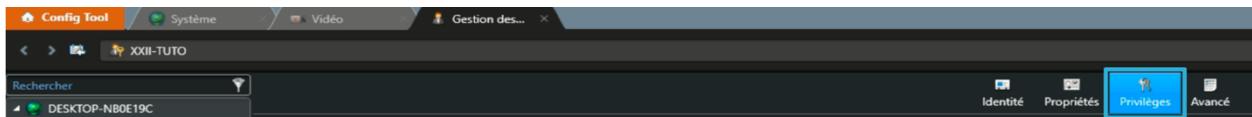
- Une fenêtre de résumé s'ouvre. C'est l'étape de la vérification et de la validation des informations. Si elles sont exactes, cliquer sur "Créer".



- Félicitations, l'utilisateur "XXII" est créé !
 - Retrouver dans l'arborescence des comptes, sur la gauche, le compte, sous > "ServerName" > Administrateurs (EN = Administrators) > XXII



- Vérifier que l'utilisateur a accès au WebSDK en cliquant sur "Privilèges".



- Vérifier dans la liste si l'option accès au WebSDK est bien activée.

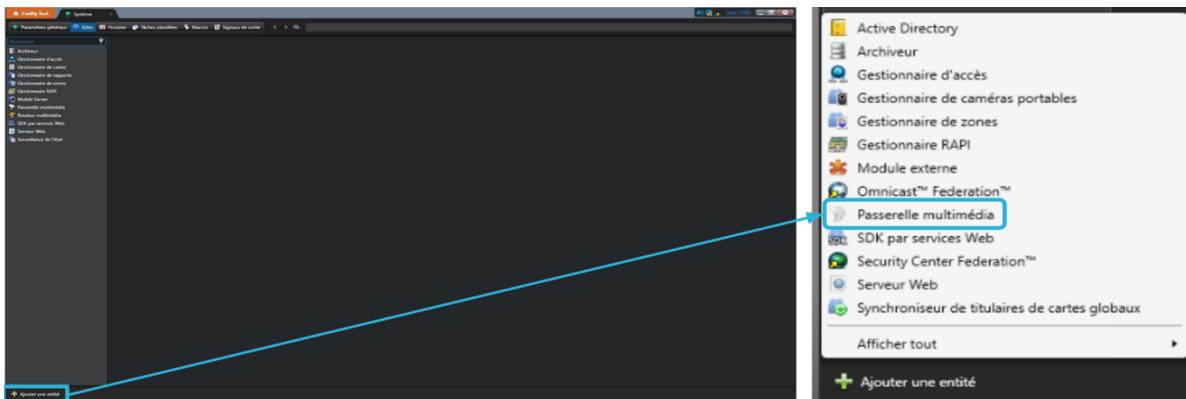
Privilèges	Autoriser	Refuser	Non défini	Hérite de
▲ Tous les privilèges	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	
▲ Privilèges d'applications	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	
Config Tool	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Administrateurs
Security Desk	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Administrateurs
Web Client	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Administrateurs
SDK Se connecter avec le SDK	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	Administrateurs
Synchroniseur de titulaires de cartes glo	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Administrateurs
Federation™	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Administrateurs
Patroller	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Administrateurs
Genetec™ Update Service	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Administrateurs
▶ Privilèges généraux	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
▶ Privilèges administratifs	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
▶ Privilèges de tâches	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	
▶ Privilèges sur les actions	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	

4 - Vérification des paramètres GENETEC : activer la passerelle multimédia

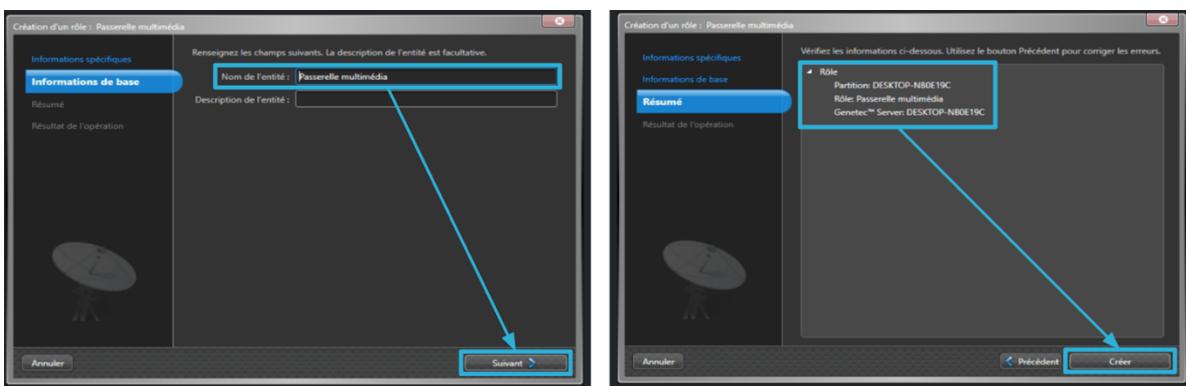
- Ouvrir le "Config Tool", Cliquer sur "système" puis sur "rôles", pour activer la passerelle multimédia.

The image shows two screenshots of the Config Tool interface. The left screenshot shows the main dashboard with various icons for administration, operation, and maintenance. The right screenshot is a zoomed-in view of the 'Système' section, which includes 'Paramètres généraux', 'Macros', 'Rôles' (highlighted with a blue box), 'Horaires', and 'Tâches planifiées'. The 'Rôles' option is specifically highlighted.

- La page “système” s’ouvre. En bas à gauche, cliquer sur le bouton “ajouter une entité” puis cliquer dans la liste sur “passerelle multimédia”.



- Une fenêtre “création d’un rôle” s’ouvre. Conserver le nom de l’entité par défaut en “passerelle multimédia” et cliquer sur “suivant”.
- Une page résumant le rôle s’affiche, cliquer sur “créer”. Félicitations, la passerelle multimédia est créée dans la liste des rôles.

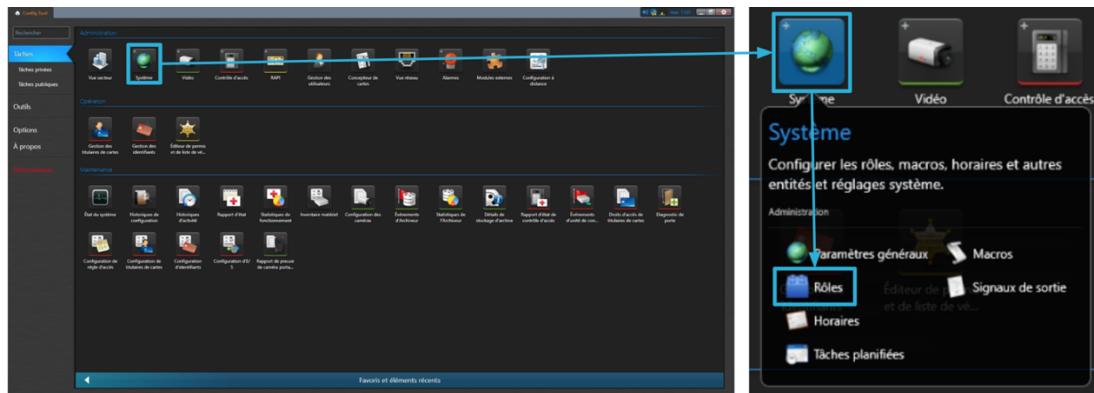


- Désactiver l’authentification de la passerelle multimédia. Sélectionner “Passerelle Multimédia” puis “Propriétés” et vérifier que le “Service d’authentification” est désactivé.
 - Si cette option n’est pas désactivée, XXII CORE REAL TIME ne sera pas en mesure de récupérer les flux.

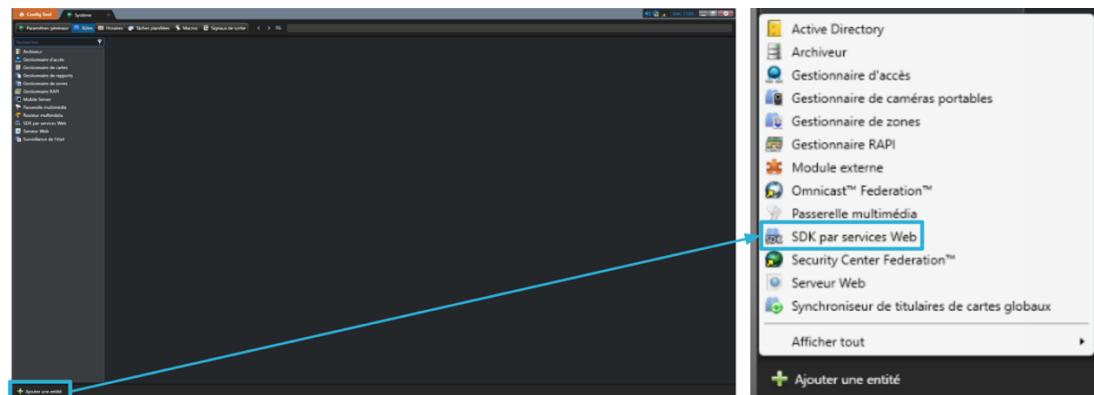


5 - Vérification des paramètres GENETEC : Activer le Web SDK

- Ouvrir le “Config Tool”, cliquer sur “système” puis cliquer sur “rôles” pour activer le “Web SDK”.**



- La page “système” s’ouvre. En bas à gauche, cliquer sur le bouton “ajouter une entité” puis cliquer dans la liste sur “SK par services Web”.**



- Une fenêtre “création d’un rôle” s’ouvre. Conserver le nom de l’entité par défaut en “SDK par services Web” et cliquer sur “suivant”.**
- Une page résumant le rôle s’affiche, cliquer sur “créer”. Félicitations, votre “WebSDK” est créé dans la liste des rôles.**



- **Pour terminer l'installation, rendez-vous dans les paramètres de pare-feu avancés de Windows pour ajouter un port de trafic entrant manuellement. En suivant le chemin suivant :**
 - Paramètres
 - Réseau et internet
 - Pare feu Windows
 - Paramètres avancés
 - Règles de trafic entrant
 - Nouvelles règles

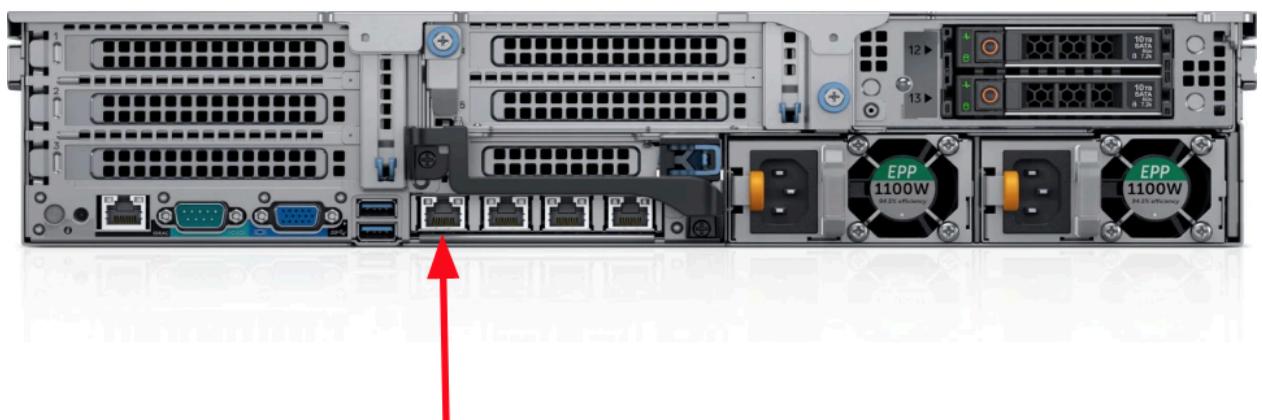
II - Installation physique dans la baie

1 - Liste pré-requis avant installation : version R1 2021 du XProtect Corporate

Operating System	
Microsoft® Windows® 8.1 Pro (64 bit)	Microsoft® Windows® Server 2012 (64 bit): Standard and Datacenter
Microsoft® Windows® 8.1 Enterprise (64 bit)	Microsoft® Windows® Server 2012 R2 (64 bit): Standard and Datacenter
Microsoft® Windows® 10 Pro (64 bit)	Microsoft® Windows® Server 2016 (64 bit): Essentials, Standard and Datacenter
Microsoft® Windows® 10 Enterprise (64 bit)	Microsoft® Windows® Server 2019 (64 bit): Essentials, Standard and Datacenter
Microsoft® Windows® 10 IoT Enterprise LTSB (Long-Term Servicing Branch)2016 (version 1607 or later)	To run clustering/failover management servers, you need a Microsoft® Windows® Server 2012/2012 R2 Standard or Datacenter edition, Microsoft® Windows® Server 2016 Standard or Datacenter edition, or a Microsoft® Windows® Server 2019 Standard or Datacenter edition
Microsoft® Windows® 10 IoT Enterprise, version 1803 or later (64 bit), IoT Core	

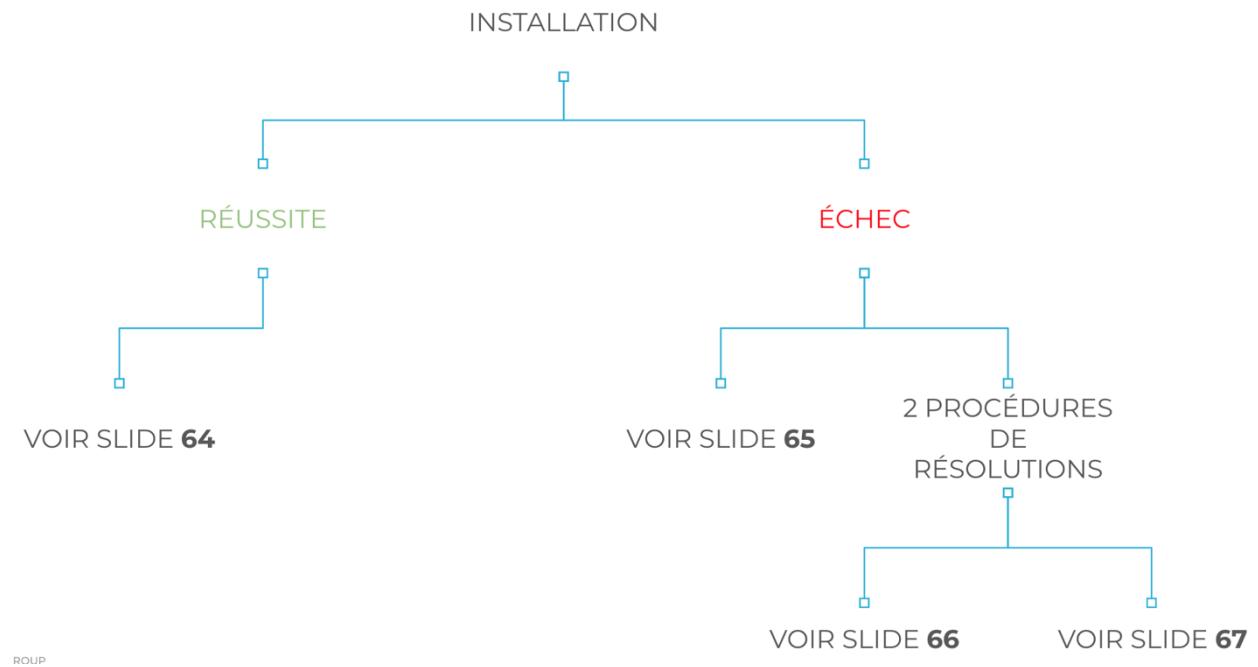
2 - Étape 1: serveur et baie de serveurs

- **Racker** le serveur XXII Core dans la baie informatique “dédiée” (**19** - **Minimum. 800 de profondeur**).
 - **Raccorder** les alimentations électriques (les 2).
 - **Raccorder** le câble ethernet en sortie de serveur sur la prise ENO1 (gauche) sur le VLAN VMS.
 - **Allumer** la machine.



3 - Étape 2 : serveur et communication

- **Ouvrir** un terminal sur un autre ordinateur et sur le même VLAN pour pinger le serveur.
 - Sur Windows :
 - **Touche Windows**
 - **Taper “cmd”**
 - **Touche entrée**
 - Sur Mac :
 - **command + espace**
 - **Taper “terminal”**
 - **Ouvrir ‘terminal’**
- **Lancer** la commande « ping \$IP_Server ».
 - Exemple : ping 192.168.1.100
- **Si le serveur** réponds au ping, alors celui-ci est correctement raccordé au bon VLAN.



- **Étape 2 (suite) :** serveur et communication - réussite

```
nathan@xxii:~$ ping 192.168.1.100
PING 192.168.1.133 (192.168.1.133) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=0.037 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.047 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=0.069 ms
```

- **Étape 2 (suite) :** serveur et communication - échec de communication

```
nathan@xxii:~$ ping 192.168.1.100
PING 192.168.1.100 (192.168.1.250) 56(84) bytes of data.
From 192.168.1.99 icmp_seq=1 Destination Host Unreachable
From 192.168.1.99 icmp_seq=2 Destination Host Unreachable
From 192.168.1.99 icmp_seq=3 Destination Host Unreachable
From 192.168.1.99 icmp_seq=4 Destination Host Unreachable
```

- **Étape 2 (suite) :** serveur et communication - vérification de la configuration ip

```
xxii@node1:~$ ifconfig | more
cni0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1450
    inet 10.233.64.1 netmask 255.255.255.0 broadcast 10.233.64.255
        inet6 fe80::bc6b:64ff:fe57:eedf prefixlen 64 scopeid 0x20<link>
            ether 6b:64:57:ee:df txqueuelen 1000 (Ethernet)
            RX packets 106170290 bytes 1565761646558 (1.5 TB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 122917347 bytes 1580935517151 (1.5 TB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

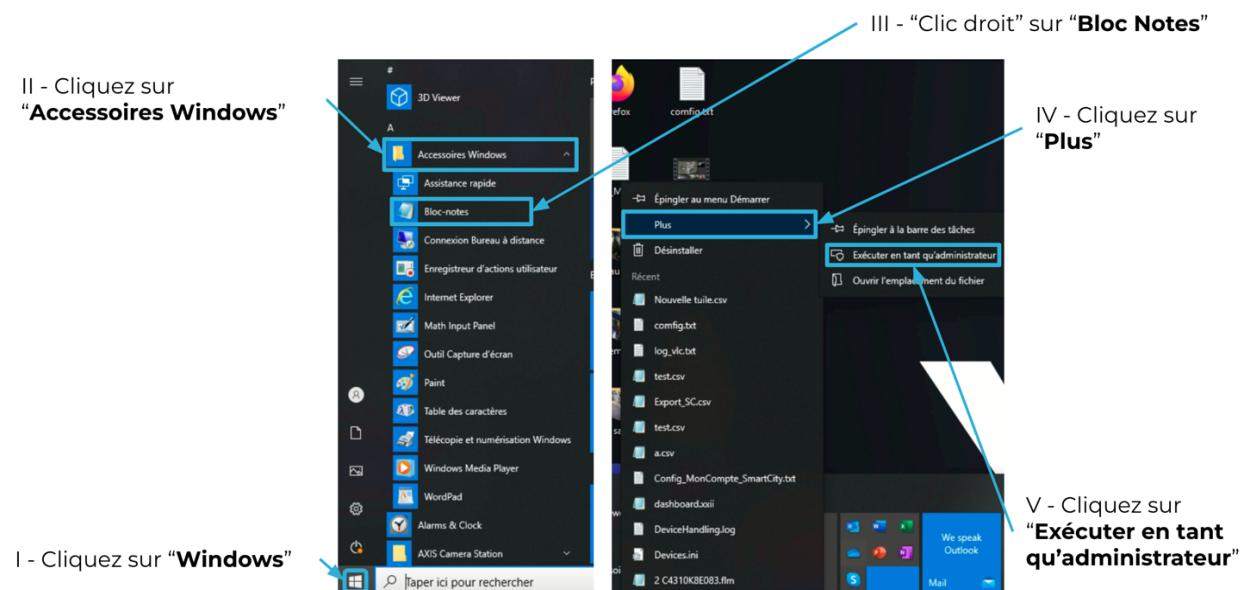
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.255.0 broadcast 172.17.255.255
        inet6 fe80::42:ffff:feb0:f456 prefixlen 64 scopeid 0x20<link>
            ether 02:42:df:b0:f4:56 txqueuelen 0 (Ethernet)
            RX packets 158 bytes 42404 (42.4 KB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 134 bytes 43769 (43.7 KB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

en0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
        inet6 fe80::b67a:1fff:fea4:12f4 prefixlen 64 scopeid 0x20<link>
            ether b4:7a:f1:a4:12:f4 txqueuelen 1000 (Ethernet)
            RX packets 31381687 bytes 1701662963 (17.0 GB)
            RX errors 0 dropped 101343 overruns 0 frame 0
            TX packets 6604058 bytes 2231936114 (2.2 GB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
            device interrupt 16
```

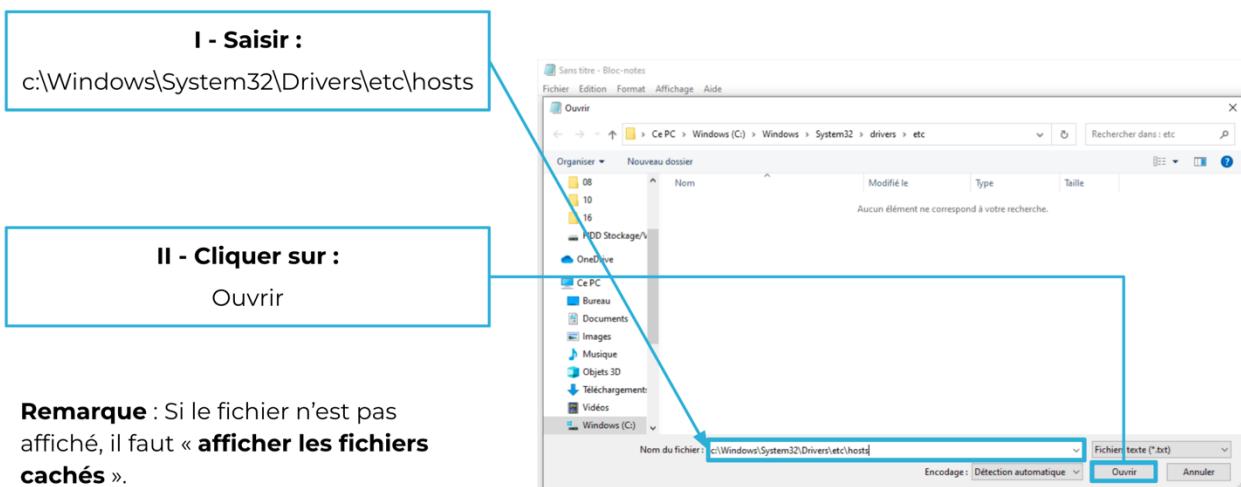
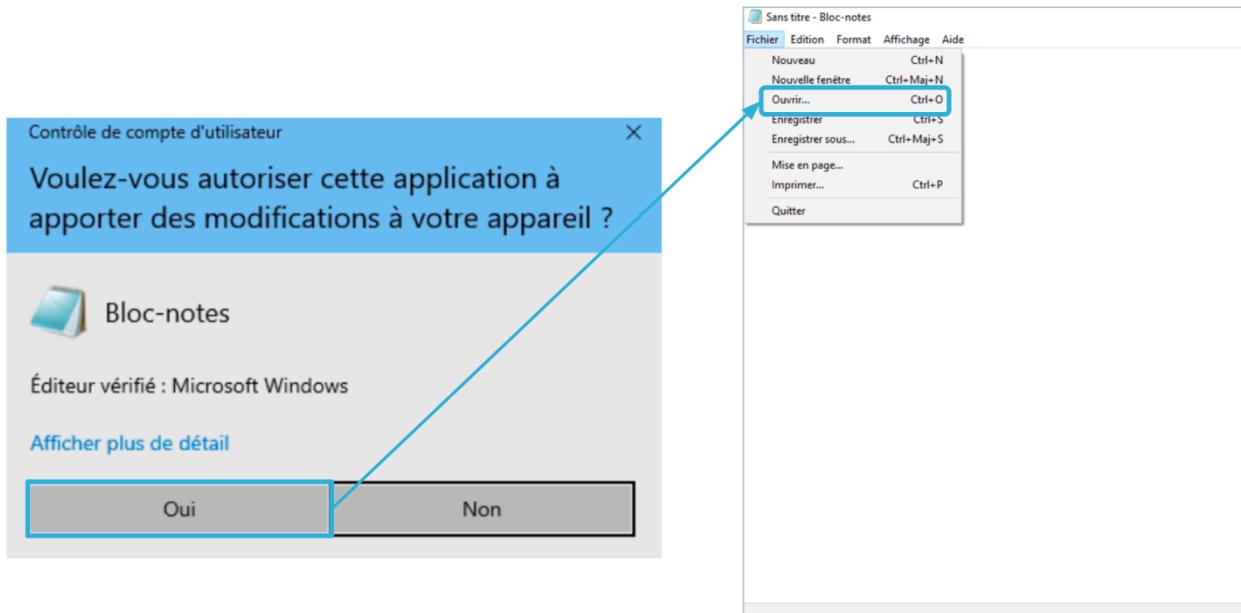
- **Étape 2 (fin) :** serveur et communication - vérification du netplan

```
xxii@node1:~$ cat /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    eno1:
      addresses: [192.168.1.100/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4]
      dhcp4: false
      dhcp6: false
  version: 2
```

4 - Étapes 3 : les ingress - ajout & méthodes (Windows)



- Cliquer sur “**Oui**” puis sur “**Ouvrir**”



- **Le fichier host** est maintenant **ouvert**, il suffit maintenant de **copier coller les ingress** à l'intérieur.
 - **Exemple :** 192.168.1.100_
 - smartcity.xxii-core.io smartcity.backend.xxii-core.io
smartcity.gateway.xxii-core.io smartcity.grafana.xxii-core.io
smartcity.kibana.xxii-core.io smartcity.prometheus.xxii-core.io
smartcity.alertmanager.xxii-core.io smartcity.results.xxii-core.io
- **Cliquer** sur **ctrl+s** ou sur **sauvegarder**
- **Fermer** le fichier.

```

hosts - Bloc-notes
Fichier Edition Format Affichage Aide
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#   102.54.94.97  rhino.acme.com    # source server
#   38.25.63.10   x.acme.com       # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1    localhost
#   ::1          localhost

#####
### MACHINE SMARTCITY - Client #####
#SmartCity#
192.168.1.69 smartcity.xxii-core.io smartcity.gateway.xxii-core.io smartcity.backend.xxii-core.io smartcity.grafana.xxii-core.io smartcity.kibana.xxii-core.io smartcity.prometh

```

Remarques : Il y a un espace entre l'adresse IP et chaque URL.

- **Saisir** la commande : sudo nano /etc/hosts
- **Cliquer sur “entrer”**
- **Entrer** votre “**mot de passe**” (Note : le mot de passe ne s'affiche pas à la saisie, vous tapez à “l'aveugle”).
- **Cliquer sur “entrer”**
- **Remarque** : Quand vous tapez des caractères rien ne s'affiche à l'écran, c'est normal c'est une question de sécurité.

```
nathan@xxii:~$ sudo nano /etc/hosts
```

```
Last login: Mon Oct 25 17:02:48 on ttys000
```

```
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
MacBook-Pro-de-Milane:~ milanecalderan$ sudo nano /etc/hosts
Password:*
```

- **Sauter** une ligne, et copier coller les ingress à la suite.
- **Remarques** : Il y a un espace entre l'adresse IP et chaque URL.

```

127.0.0.1      localhost
127.0.1.1      xps

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

#Node1
192.168.1.100 node1

#SmartCity
192.168.1.100 smartcity.xxii-core.io smartcity.backend.xxii-core.io smartcity.gateway.xxii-core.io
smartcity.results.xxii-core.io smartcity.kibana.xxii-core.io smartcity.alertmanager.xxii-core.io

```

- **Étape 3 bis : Ajouter les Ingress dans le DNS du réseau local**
 - Ajouter les ingress sur le serveur DNS
 - **Récupérer les ingress en se connectant en SSH au serveur et en tapant la commande :** kubectl get ingress -A

```

xxii@node1:~$ kubectl get ingress -A
NAMESPACE   NAME          CLASS      HOSTS                               ADDRESS        PORTS   AGE
default     platform-resultapi <none>    smartcity.results.xxii-core.io  10.233.26.238  80     174d
default     platform-web-frontend <none>   smartcity.xxii-core.io       10.233.26.238  80     174d
default     platform-web-gateway  <none>   smartcity.gateway.xxii-core.io 10.233.26.238  80     131d
default     processor-debug     <none>   smartcity.debug.xxii-core.io  10.233.26.238  80     43d
monitoring  monitoring-efk-kb- http <none>  smartcity.kibana.xxii-core.io  10.233.26.238  80     174d
monitoring  monitoring-prometheus-oper-alertmanager <none> smartcity.alertmanager.xxii-core.io 10.233.26.238  80     174d
monitoring  monitoring-prometheus-oper-prometheus   <none>  smartcity.prometheus.xxii-core.io 10.233.26.238  80     174d
monitoring  monitoring-prometheus-operator-grafana   <none>  smarcity.grafana.xxii-core.io  10.233.26.238  80     174d

```

5 - Étape 4 : activation des licences XXII CORE

- **Saisir** l'URL suivante : ipdelamachine:1947
- **Cliquer** sur **Update/Attach** pour ouvrir cette page.

The screenshot shows the Gemalto Admin Control Center Help page. The URL in the browser bar is 192.168.1.133:1947. On the left, there's a sidebar with various options: Sentinel Keys, Products, Features, Sessions, Update/Attach (which is highlighted), Access Log, Configuration, Diagnostics, Help, and About. The main content area is titled "Admin Control Center Help" and contains a welcome message, notes about language selection, and details about monitoring and managing protection keys. It also lists actions like detaching, cancelling, and installing updates.

- **Sélectionner “choisir un fichier” et “charger”** le fichier “→ .v2c qui vous a été transmis lors de la souscription de contrat. Félicitations, **XXII CORE est activé !**

The screenshot shows the "Update/Attach License to node1" page. The left sidebar includes the "Update/Attach" option. The main area is titled "Update/Attach License to node1" and contains a "Apply File" section with a file selection dialog. The dialog shows "Choisir un fichier" and "Aucun fichier choisi". Below the dialog, a list of file types that can be applied is provided, including V2C, V2CP, H2R, R2H, H2H, and ID files, along with their descriptions.

6 - Étape 5 : mise en action de XXII Core

- **Ouvrir** la page de configuration web de XXII Core
- **Saisir** dans un navigateur internet l'adresse suivante :
 - Attention, il ne faut surtout pas oublier le port 32080, sinon l'adresse sera inaccessible
- **Identifiez-vous** en renseignant :
 - Identifiant
 - Mot de passe
- **Si vous avez égaré ces informations**, vous pouvez appeler le support XXII : 01 84 20 48 22

