

UNIVERSITE AUBE NOUVELLE



INSTITUT SUPERIEUR D'INFORMATIQUE ET DE GESTION

DEPARTEMENT HIGH TECH (HT)

RAPPORT DE STAGE EN VUE DE L'OBTENTION DE LA LICENCE

OPTION : Technologie des Réseaux et Systèmes Informatiques

Thème :

*Étude et mise en place d'un système d'authentification
dans le réseau IP du Centre MURAZ*

Présenté et soutenu par : ZOURE Abdramane. Le : 26 Mars 2024

PRESIDENT DU JURY

Dr. KIENTEGA Raoul

Enseignant chercheur

<https://orcid.org/0009-0002->

[8619-5736](https://orcid.org/0009-0002-8619-5736)

DIRECTEUR DE MEMOIRE

M. TRAORE Tiémogo

Enseignant à l'Université Aube
Nouvelle

MAITRE DE STAGE

M. ZOUNGRANA Moumouni

Responsable de la section
informatique au Centre MURAZ

Année Académique 2022-2023

SOMMAIRE

AVANT-PROPOS.....	III
DEDICACE	V
REMERCIEMENTS.....	VI
RESUME.....	VII
ABSTRAT	VIII
LISTE DES TABLEAUX	IX
LISTE DES FIGURES	X
LISTE SIGLES ET ABREVIATIONS.....	XII
INTRODUCTION GENERALE	1
PROBLEMATIQUE.....	3
CHAPITRE 1 : CONTEXTE DU PROJET.....	4
1.1 Introduction.....	5
1.2 Présentation du Centre MURAZ	5
1.3 Contexte et Justification du projet	11
1.4 Objectifs de l'Étude	14
1.5 Conclusion	16
CHAPITRE 2 : ANALYSE DES BESOINS EN SECURITE.....	18
2.1. Introduction.....	19
2.2. Identification des Besoins de Sécurité	19

2.3.	Évaluation des Risques.....	22
2.4.	Conclusion	34
CHAPITRE 3 : SELECTION DE LA SOLUTION D'AUTHENTIFICATION		36
3.1.	Introduction	37
3.2.	Revue des Solutions Disponibles [5]	37
3.3.	Choix de la Solution d'Authentification.....	45
3.4.	Conclusion.....	48
CHAPITRE 4 : CONCEPTION DU SYSTHEME D'AUTHENTIFICATION		49
4.1.	Introduction	50
4.2.	Architecture du Système d'Authentification	50
4.3.	Protocoles et Technologies Utilisés	54
4.4.	Conclusion.....	71
CHAPITRE 5 : MISE EN ŒUVRE DU SYSTHEME D'AUTHENTIFICATION.....		72
5.1.	Introduction	73
5.2.	Installation et Configuration.....	73
5.3.	Tests et Validation.....	103
5.4.	Bilan	106
5.5.	Conclusion.....	107
CONCLUSION GENERALE		108
REFERENCES		XIV

AVANT-PROPOS

L'institut Supérieur de l'Informatique et de Gestion (ISIG) est une société à responsabilité limitée (SARL) créé en 1992 et agréé par l'Etat par arrêté n°92-125/ESSRS du 21 Octobre 1992, ces modificatifs arrêté 2010-335/MESSRS/ETFP/CAB du 11 Octobre 2010 portant modification des statuts de l'ISIG INTERNATIONAL.

Un campus a été ouverte à Bobo-Dioulasso dans le cadre de la décentralisation de son enseignement qui donne à l'institut deux campus, celui de Ouagadougou et celui de Bobo-Dioulasso.

Plusieurs textes ont permis l'évolution de ISIG INTERNATIONAL qui est la première université privée au Burkina Faso devenu ensuite UNIVERSITE AUBE NOUVELLE (U-AUBEN) par autorisation n°20120000344/MESS/SG/DGESR/DIESPR du 17 Février 2012. Organisée sur deux (02) campus, Ouagadougou et Bobo-Dioulasso, elle comprend :

- Quatre (04) Unités de Formation et de Recherche (UFR) : Sciences et Technologies, Sciences Économiques et de Gestion, Sciences Juridiques et Politiques, Lettres – Langues et Sciences Humaines ;
- Deux (02) Instituts : Institut Supérieur d'Informatique et de Gestion (ISIG), Institut des Métiers de la Communication, du Journalisme, de l'Audio-Visuel et du Cinéma (IMCJAC) ;
- Elle compte plusieurs laboratoires pour une bonne formation pratique : Laboratoire de Sciences biologiques appliquées, Laboratoire de Génie civil et de Géologie et Mines, Laboratoire d'Informatique et Laboratoire d'Architecture ; Laboratoire génie civil et en informatique
- Elle anime deux centres de Culture américaine : le Centre Américain de Langues (ALC), et l'American Corner (AC) ;
- Elle entretient de nombreux partenariats aux niveaux national, régional et international en vue de faciliter la poursuite de votre formation.

Les diplômes délivrés ont les grades de DUT, Licence, Master et Doctorat. Ils sont en majorité reconnus par la CAMES, cette reconnaissance est due à la pertinence des programmes d'études proposés ainsi qu'à l'usage d'équipements de pointe pour une formation adéquate. U-

AUBEN propose par ailleurs aussi bien des formations en continue que des formations à distance. Le système LMD est adopté depuis la rentrée académique 2006-2007. Le premier cycle de ce système dure trois ans à l'issue duquel un mémoire est redirigé et soutenu devant un jury et sanctionné par un Licence professionnelle en Technologies des Réseaux et systèmes pour notre cas.



DEDICACE

À mon père, ma maman, toute ma famille, mes très chères amies et amis, mes professeurs de l'Université Aube Nouvelle, ainsi qu'à tous ceux et celles qui m'ont soutenu tout au long de ce parcours,

Je tiens à exprimer ma profonde gratitude envers vous pour votre soutien inconditionnel durant mon parcours de licence.

Vos encouragements et vos conseils m'ont été d'une aide inestimable tout au long de ce cheminement académique. Votre présence bienveillante a été une source de motivation et de soutien, me permettant de surmonter les défis et d'atteindre mes objectifs.

Je vous dédie ce mémoire en témoignage de ma reconnaissance et de ma gratitude sincère pour votre impact positif sur mon parcours universitaire

REMERCIEMENTS

Nous tenons ici à témoigner notre reconnaissance à Dieu et notre gratitude aux entités et aux personnes sans lesquelles ce projet n'aurait jamais vu le jour :

- Nous exprimons nos vifs remerciements à l'endroit de toute l'équipe pédagogique de l'Université Aube Nouvelle (U-AUBEN) et des intervenants professionnels, qui ont assuré avec dévouement notre formation.
- Nous remercions également la Direction Technique du Centre MURAZ, ainsi que toute son équipe, pour l'expérience enrichissante et pleine d'intérêt qu'ils nous ont fait vivre durant cette période de stage.

Nous tenons à remercier tout particulièrement et à témoigner toute notre reconnaissance aux personnes suivantes :

- **M. Tiémogo TRAORE**, Enseignant à l'U-AUBEN, le superviseur de ce travail ;
- **M. Moumouni ZOUNGRANA**, ingénieur informaticien au Centre MURAZ, chef de Section informatique, maître de stage pour son encadrement et sa disponibilité.

Nous ne saurions terminer sans exprimer notre profonde gratitude à nos familles respectives, en particulier nos parents, pour leurs prières, leurs soutiens multiformes, leur amour, leur patience durant tout notre cursus. Ce rapport n'est qu'un fruit de tous les combats et sacrifices qu'elles ont eus à mener pour nous.

Enfin nous adressons nos remerciements à tous nos amis, camarades de classes et tous nos proches qui nous ont soutenus d'une manière ou d'une autre pour la bonne réalisation de ce travail.



RESUME

Ce mémoire présente une étude approfondie suivie de la mise en place d'un système d'authentification au sein du réseau IP du Centre MURAZ. L'objectif principal est d'améliorer la sécurité des données et des utilisateurs tout en optimisant l'accès au réseau. La première partie du mémoire se concentre sur une analyse détaillée des différents types d'attaques et de menaces potentielles auxquels le réseau IP du Centre MURAZ est exposé. Cette analyse permet de comprendre les vulnérabilités existantes et les risques encourus en l'absence d'un système d'authentification robuste. Ensuite, une revue exhaustive des technologies d'authentification disponibles est effectuée, en mettant l'accent sur leurs avantages, leurs inconvénients et leur pertinence pour le contexte du Centre MURAZ. Des méthodes telles que l'authentification à facteur unique, l'authentification à deux facteurs, l'authentification unique et l'authentification MFA sont examinées en détail. Sur la base de cette analyse, une architecture de système d'authentification est proposée, adaptée aux besoins spécifiques du Centre MURAZ. Cette architecture prend en compte les contraintes liées à l'infrastructure existante tout en garantissant un niveau élevé de sécurité et de convivialité pour les utilisateurs. La mise en œuvre pratique du système d'authentification est ensuite décrite, mettant en lumière les étapes de déploiement, les configurations requises et les tests de fonctionnalité effectués. Des mesures de surveillance et de maintenance sont également abordées pour assurer la continuité et l'efficacité du système dans le temps.

Ce mémoire démontre l'importance cruciale d'un système d'authentification efficace pour garantir la sécurité et la fiabilité du réseau IP du Centre MURAZ. Il offre des recommandations pratiques pour les professionnels de la sécurité informatique et les administrateurs réseau cherchant à renforcer la protection des infrastructures critiques contre les cybermenaces.



ABSTRACT

This thesis presents an in-depth study followed by the implementation of an authentication system within the IP network of the MURAZ Center. The main objective is to enhance data and user security while optimizing network access. The first part of the thesis focuses on a detailed analysis of various types of attacks and potential threats to which the MURAZ Center IP network is exposed. This analysis helps understand existing vulnerabilities and risks in the absence of a robust authentication system. Subsequently, a comprehensive review of available authentication technologies is conducted, emphasizing their advantages, disadvantages, and relevance to the MURAZ Center context. Methods such as single-factor authentication, two-factor authentication, single sign-on, and MFA authentication are examined in detail. Based on this analysis, an authentication system architecture is proposed, tailored to the specific needs of the MURAZ Center. This architecture considers constraints related to existing infrastructure while ensuring a high level of security and user-friendliness. The practical implementation of the authentication system is then described, highlighting deployment steps, required configurations, and conducted functionality tests. Monitoring and maintenance measures are also addressed to ensure the system's continuity and effectiveness over time. This thesis demonstrates the crucial importance of an effective authentication system in ensuring the security and reliability of the MURAZ Center IP network. It provides practical recommendations for cybersecurity professionals and network administrators seeking to enhance protection of critical infrastructures against cyber threats.

LISTE DES TABLEAUX

Tableau 1: Tableau comparatif des solutions	44
Tableau 2: Comparaison entre 2FA et SSO	46
Tableau 3: Les systèmes compatibles avec UserLock 12.0	73
Tableau 4: Estimation des coûts de réalisation	77

LISTE DES FIGURES

Figure 1: Organigramme du Centre MURAZ (Source Centre MURAZ)	10
Figure 2: Principe de l'authentification à double facteurs (2FA) [5].....	39
Figure 3: Architecture du système d'authentification à 2FA [12].....	54
Figure 4: Une clé USB U2F [6]	60
Figure 5: Architecture de déploiement [8]	76
Figure 6: Page d'accueil de configuration UserLock	79
Figure 7: Type de serveur.....	80
Figure 8: Zone à protéger par Userlock.....	81
Figure 9: Identification du compte de dépersonnalisation	82
Figure 10: Fin de configuration	83
Figure 11: Page d'accueil UserLock	84
Figure 12: Choix de la base de données	85
Figure 13: Connexion à la base de données.....	86
Figure 14: Installation des agents	87
Figure 15: Progression de l'installation des agents	88
Figure 16: Liste des Agents installés	89
Figure 17: Déploiement automatique des agents	90
Figure 18: Accueil de comptes protégés.....	92
Figure 19: Choix du mode de Création du compte	93
Figure 20: Choix du type de compte à protéger.....	93
Figure 21: Sélection du compte AD à protéger.....	94
Figure 22: Sélection de l'objet.	94
Figure 23: Création d'un compte protégé temporaire.....	95
Figure 24: Liste des comptes protégés	96

Figure 25: Tableau de bord de l'authentification multi facteur.....	97
Figure 26: Configuration de "Demander de l'aide"	98
Figure 27: Configuration des méthodes MFA.....	99
Figure 28: Configuration des codes de récupération.....	100
Figure 29: Activation de la MFA pour les comptes protégés.....	102
Figure 30: Paramétrage de l'option ignorer	103
Figure 31: Diagramme réel.....	107
Figure 32: Configuration de l'authentification multifacteur	104
Figure 33: Google authenticator.....	104
Figure 34: Ajouter un compte	105
Figure 35: Code MFA.....	105
Figure 36: Saisi de code.....	106

LISTE SIGLES ET ABREVIATIONS

2FA	Two-Factor Authentication
AD	Active Directory
AD DS	Active Directory Domain Services
CHAP	Challenge Handshake Authentication Protocol
CPU	Central Processing Unit
DB	Database
DDoS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
D.I.C	Disponibilité, Intégrité et Confidentialité
DLP	Data Loss Prevention
DNS	Domain Name System
EAP	Extensible Authentication Protocol
FIDO	Fast Identity Online
GHz	Gigahertz
HIPAA	Health Insurance Portability and Accountability Act
HMAC	Hash-Based Message Authentication Code
HOTP	HMAC-Based One-Time Password
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
IIS	Internet Information Services
IP	Internet Protocol
MD5	Message Digest 5
Mdb	Microsoft database

MFA	Authentication Multi-Factors
MitM	Man-in-the-Middle
MS Access	Microsoft Access
NFC	Near Field Communication
NPS	Network Policy Server
OWASP	Open Web Application Security Project
PAP	Protocole d'Authentification par mot de Passe
QR	Quick Response Code
RAM	Random Access Memory
RDP	Remote Desktop Protocol
RGPD	Règlement General sur la protection des données
S.I	Système Information
SIM	Subscriber Identity Module
SMB	Server Message Block
SMS	Short Message Service
SSL/TLS	Secure Sockets Layer/ Transport Layer Security
SSO	Authentication Unique
SQL	Structured Query Language
TCP	Transmission Control Protocol
TOTP	Time-Based One-Time Password
U2F	Universal 2 nd Factor
USB	Universal Serial Bus
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WebAuthn	Web Authentication

INTRODUCTION GENERALE

Dans un contexte où les données sensibles et les ressources numériques sont de plus en plus exposées à des menaces de sécurité, la nécessité de mettre en place des systèmes d'authentification robustes et fiables devient primordiale. C'est dans cette optique que s'inscrit ce mémoire, qui se concentre sur le thème « Etude et mise en place d'un système d'authentification dans le réseau IP du Centre MURAZ ».

Le Centre MURAZ, en tant qu'institution de recherche en santé, gère une quantité importante de données médicales, de recherches et d'informations confidentielles. La sécurité de ces données est essentielle non seulement pour préserver la confidentialité des patients et des chercheurs, mais aussi pour assurer le bon fonctionnement des activités de l'institution. Face à ces enjeux, ce mémoire se propose d'analyser les besoins spécifiques en matière de sécurité du Centre MURAZ, en mettant en lumière les risques potentiels auxquels le réseau IP de l'institution est exposé. Il vise également à explorer les différentes méthodes et technologies d'authentification disponibles, dans le but de sélectionner celle qui répond le mieux aux exigences actuelles de sécurité et d'efficacité.

Au-delà de l'aspect technique, ce mémoire s'intéresse également aux implications organisationnelles et opérationnelles de la mise en place d'un système d'authentification. En effet, un tel projet nécessite une collaboration étroite entre les équipes informatiques, les responsables de la sécurité et les utilisateurs finaux, afin d'assurer une adoption réussie et un fonctionnement optimal du système.

Ce rapport s'articule autour de cinq (05) chapitres. Le premier chapitre présente le contexte du projet. Le deuxième concerne l'analyse des besoins en sécurité. Le troisième présente la sélection de la solution d'authentification. Le

quatrième chapitre traite la conception du système d'authentification et le cinquième porte sur la mise en œuvre du système d'authentification. Nous terminons par une conclusion générale qui récapitule les principales observations concernant le travail réalisé.



PROBLEMATIQUE

Le Centre MURAZ, situé au cœur de notre communauté, est une référence en matière de santé publique et de recherche médicale depuis de nombreuses années. Son réseau IP est le fondement technologique de ses activités, supportant une variété de services allant de la gestion des dossiers médicaux à la communication entre les praticiens de la santé.

Pourtant, face à l'évolution constante des menaces informatiques et à l'augmentation de la sensibilité des données médicales, la nécessité d'une mise en place d'un système d'authentification solide au sein du réseau IP du Centre Muraz est devenue impérative. Les risques potentiels liés à la vulnérabilité actuelle du réseau soulignent l'urgence d'une intervention appropriée.

L'objectif principal de cette étude est d'explorer les mécanismes, les technologies et les meilleures pratiques pour concevoir, implémenter et gérer un système d'authentification efficace, adapté aux besoins spécifiques du Centre MURAZ, tout en garantissant la sécurité et la confidentialité des données médicales.

CHAPITRE 1 : CONTEXTE DU PROJET

1.1 Introduction

L'Université Aube Nouvelle (U-AUBEN) inclut dans le programme de formation de ses étudiants de troisième année, un stage pratique obligatoire de trois (03) mois minimum ; ce stage ayant pour objectif de familiariser l'étudiant avec les exigences d'un milieu de travail, nous nous sommes tournés vers le Centre MURAZ qui a bien voulu nous en accorder un. Dans ce chapitre, il sera question d'abord de présenter l'ESI notre structure de formation. Ensuite nous présenterons la SOFITEX, son historique et ses domaines d'intervention. Et, pour finir nous parlerons de notre projet, de la problématique et des résultats attendus.

1.2 Présentation du Centre MURAZ

1.2.1 Historique

Le Centre MURAZ est une institution nationale de recherche en santé, situé dans la ville de Bobo-Dioulasso sur l'avenue Mamadou KONATE. Son histoire commence en 1939 sous l'appellation Service Général Autonome de la Maladie du Sommeil (SGAMS) en tant que Centre décisionnel, sous la commande d'un médecin colonel du nom de Gaston MURAZ. En 1945, il prit le nom de Service Général d'Hygiène Mobile et de Prophylaxie (SGHMP). En 1956, il prit le nom de Centre MURAZ. Le Centre MURAZ est devenu le siège de l'Organisation de Coordination et de Coopération pour la Lutte contre les Grandes Endémies (OCCGE) qui regroupait huit (8) pays francophones de l'Afrique de l'Ouest.

Le laboratoire du paludisme du Centre MURAZ avait été érigé en Centre de référence de la chimiorésistance du paludisme. Erigé en Etablissement Public de l'Etat à caractère Administratif (EPA) le 10 mai 2001, il fut transformé en Etablissement Public de Santé en septembre 2006. Depuis juillet 2018, le Centre MURAZ est devenu une Direction Technique de l'Institut National de Santé Publique (INSP).

De sa devise RECHERCHE-FORMATION-EXPERTISE, ce Centre a trois grandes missions :

➤ La recherche dans le domaine de la santé ;

C'est la mission première et aussi la plus connue du centre. Elle est Organisée autour de quatre (04) programmes de recherche qui sont :

- Programme de **R**echerche **M**aladies **I**nfectieuses (**PR-MI**)
- Programme de **R**echerche sur les **M**aladies à **P**otentiel **E**pidémique (**PR-MPE**)
- Programme de **R**echerche sur les **P**olitiques et **S**ystèmes de **S**anté et de **C**apitalisation (**PR-PSSC**)
- Programme de **R**echerche sur la **S**anté **S**exuelle et **R**eproductive (**PR-SSR**)

➤ La formation du personnel de santé ;

Elle consiste en une participation effective à la formation du personnel de santé à travers des stages pour paramédicaux, doctorants (mémoires, thèses), post-doctorants.

➤ L'expertise : Elle consiste au renforcement des capacités et des compétences nationales de sorte à disposer sur le plan technique d'experts de haut niveau.

La définition de ses missions et son dévouement perpétuel pour les mener à bien font que le Centre se trouve souvent sollicité par des organismes tels que l'OMS pour l'animation de séminaires de formation, le contrôle de qualité de laboratoire etc.

1.2.2 Visions et objectifs

Le Centre MURAZ a pour vision d'être une référence en matière de santé publique. Pour ce faire, il s'est fixé des objectifs qui sont révisés chaque année. Pour l'année 2022, nous comptons six objectifs qui sont :

- Satisfaire au moins 90% des besoins de fonctionnement exprimés chaque année au sein du Centre MURAZ
- Assurez la satisfaction d'au moins 80% des clients (interne et externes) chaque année
- Accompagner les entités du Centre MURAZ à mettre en place /à jour la documentation qualité
- Accompagner chaque programme /laboratoire de Centre MURAZ à réaliser les activités de recherche et à publier au moins un article scientifique par an.
- Assurez l'analyse des échantillons transmis au laboratoire dans les délais spécifiés par chaque laboratoire.
- Acquérir chaque année au moins une étoile supplémentaire sur l'échelle SLIPTA à l'issu des audits internes ou externes des laboratoires.

1.2.3 Rôle du réseau IP

Le réseau IP joue un rôle essentiel pour le Centre MURAZ, comme pour toute institution ou organisation, est essentiel pour assurer la connectivité, la communication et le bon fonctionnement des systèmes informatiques et de communication :

- ✓ Communication et collaboration, le réseau IP permet au Centre MURAZ de communiquer efficacement en interne entre ses différents départements, laboratoires de recherche et bureaux administratifs. Il facilite également la

collaboration avec d'autres institutions de recherche, hôpitaux, agences de santé, universités et organisations partenaires, tant au niveau local qu'international. La communication en temps réel via le réseau IP est essentielle pour coordonner les activités de recherche, partager des données, et échanger des informations critiques ;

- ✓ Transmission de données, le Centre MURAZ effectue de nombreuses études de recherche, collecte des données épidémiologiques et génère des informations cliniques. Le réseau IP est nécessaire pour transférer ces données entre les différents systèmes informatiques, laboratoires, bases de données et serveurs de stockage. La fiabilité et la sécurité du réseau IP sont cruciales pour garantir l'intégrité des données et la confidentialité des informations sensibles ;
- ✓ Accès à des ressources externes, le réseau IP permet au Centre Muraz d'accéder à des ressources en ligne telles que des bases de données médicales, des revues scientifiques, des outils de recherche et de modélisation, et des collaborations avec des experts à l'échelle mondiale. Cela facilite la recherche, la formation et l'accès aux dernières informations médicales et scientifiques ;
- ✓ Formation et éducation, le réseau IP est utilisé pour la formation continue des professionnels de la santé, la diffusion de connaissances médicales et l'accès à des ressources éducatives en ligne ;
- ✓ Sécurité des données, le réseau IP permet de sécuriser et de protéger les données médicales sensibles, notamment les informations sur les patients et les données de recherche confidentielles du Centre. Grâce au réseau IP le Centre dispose d'une sécurité physique. En effet, pour avoir accès à la direction et aux laboratoires il faut s'authentifier avec un badge ou une empreinte digitale ;

- ✓ Surveillance épidémiologique, le réseau IP est essentiel pour la collecte en temps réel de données de surveillance épidémiologique, permettant au Centre Muraz de suivre l'évolution des maladies infectieuses dans la région, d'identifier les épidémies potentielles et de contribuer aux efforts de santé publique.

1.2.4 Organisation du Centre MURAZ

Le Centre MURAZ est dirigé par un Directeur Technique (DT).

Son organigramme se présente comme suit :

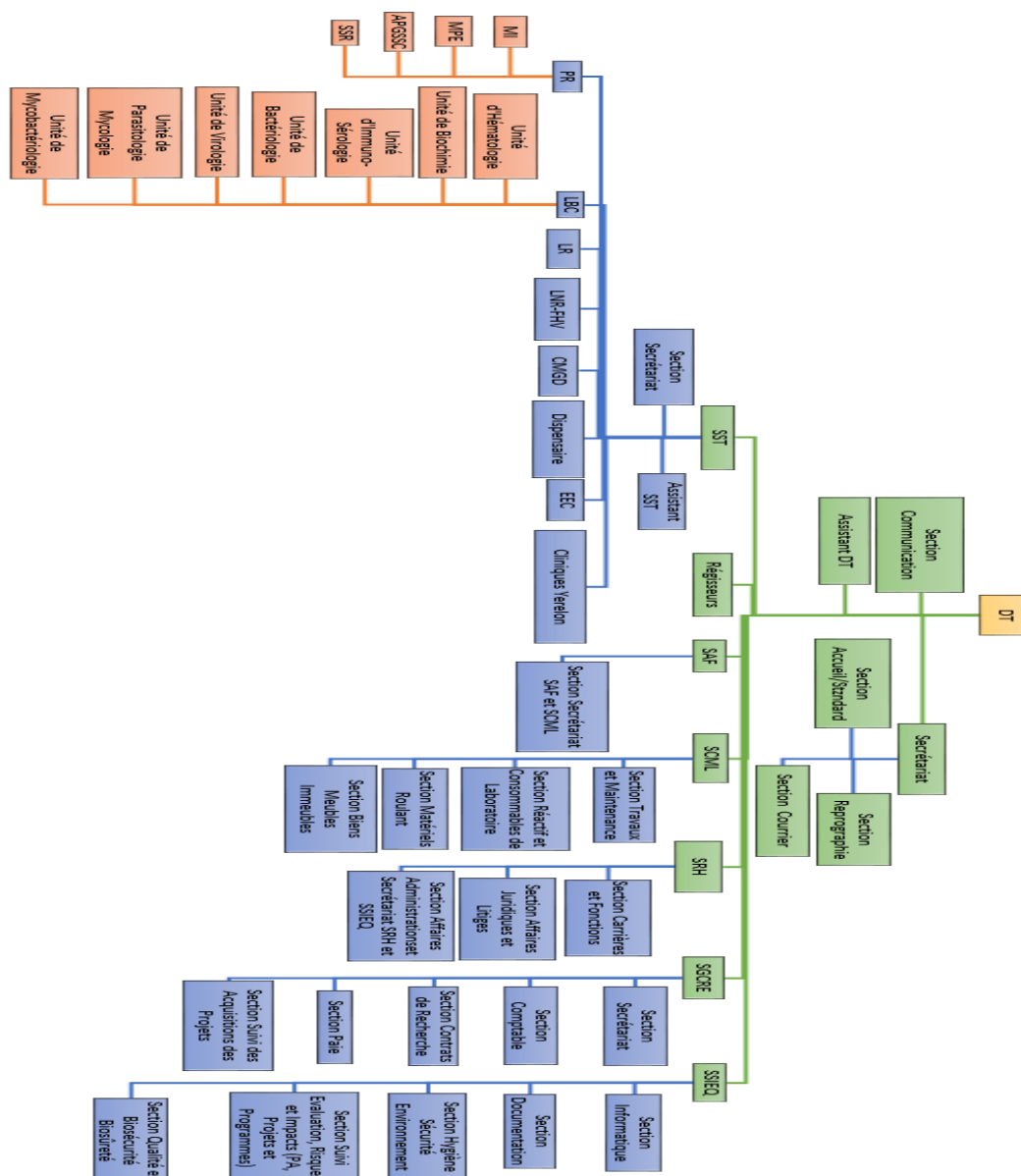


Figure 1: Organigramme du Centre MURAZ (Source Centre MURAZ)

1.3 Contexte et Justification du projet

1.3.1 Importance d'un système d'authentification solide

Un système d'authentification solide revêt une grande importance pour le Centre MURAZ, qui est un institut de recherche en santé situé à Bobo-Dioulasso, au Burkina Faso. Voici pourquoi un système d'authentification solide est crucial pour le Centre MURAZ :

- ✓ Protection des données de recherche, le Centre MURAZ mène des recherches médicales et épidémiologiques, et il peut stocker des données sensibles, notamment des informations sur les patients, des données de recherche clinique, des données épidémiologiques, etc. Un système d'authentification solide garantit que seuls les chercheurs et le personnel autorisé ont accès à ces données, protégeant ainsi la confidentialité et l'intégrité de ces informations ;
- ✓ Conformité réglementaire, le Centre MURAZ doit se conformer à des réglementations nationales et internationales en matière de protection des données et de confidentialité, notamment en ce qui concerne les données médicales et de recherche. Un système d'authentification robuste est essentiel pour respecter ces réglementations et garantir que les données sensibles sont traitées de manière appropriée ;
- ✓ Sécurité de la recherche, la recherche médicale peut impliquer des données sensibles et des informations qui, si elles tombaient entre de mauvaises mains, pourraient être utilisées de manière malveillante ou compromettre la validité des recherches. Un système d'authentification solide protège ces données contre l'accès non autorisé ;
- ✓ Gestion des ressources, le Centre MURAZ peut gérer diverses ressources, telles que des laboratoires, des équipements médicaux, des installations de recherche, etc. Un système d'authentification solide peut aider à contrôler et

à surveiller l'accès à ces ressources, garantissant qu'elles sont utilisées de manière appropriée ;

- ✓ Collaboration et partage de données, le Centre MURAZ collabore probablement avec d'autres institutions de recherche et de santé à l'échelle nationale et internationale. Un système d'authentification solide facilite le partage sécurisé de données et de résultats de recherche avec des partenaires, en veillant à ce que seules les personnes autorisées aient accès aux informations partagées ;
- ✓ Prévention de l'usurpation d'identité ; un système d'authentification solide contribue à prévenir l'usurpation d'identité et garantit que les chercheurs, les professionnels de la santé et le personnel du Centre MURAZ sont correctement identifiés avant d'accéder aux systèmes et aux données ;
- ✓ Continuité des opérations, la sécurité des systèmes informatiques et des données est essentielle pour assurer la continuité des opérations de recherche et de santé. Un système d'authentification solide protège contre les perturbations potentielles causées par des violations de sécurité.

Un système d'authentification solide est essentiel pour le Centre MURAZ afin de garantir la sécurité, la confidentialité et l'intégrité des données de recherche, de respecter les réglementations, de prévenir les risques liés à la sécurité et de maintenir la confiance des partenaires et du public dans les activités de recherche et de santé menées par l'institut.

1.3.2 Risques actuels liés à la vulnérabilité du réseau IP

Les réseaux IP, bien qu'essentiels pour la communication et la connectivité à l'échelle mondiale, sont soumis à divers risques liés à leur vulnérabilité. Voici quelques-uns des risques actuels liés à la vulnérabilité du réseau IP du Centre MURAZ :

- ✓ Sécurité de la recherche, la recherche médicale du Centre peut impliquer des données sensibles et des informations qui, si elles tombaient entre de mauvaises mains, pourraient être utilisées de manière malveillante ou compromettre la validité des recherches ;
- ✓ Falsification de paquets, avec l'accès non contrôlé au réseau du Centre, les paquets de données peuvent être falsifiés, ce qui permet aux attaquants de modifier, d'intercepter ou de perturber la communication entre les nœuds du réseau ;
- ✓ Attaques de routage, les attaques de routage visent à manipuler les tables de routage pour rediriger le trafic vers des destinations non autorisées. Cela peut entraîner la perte de données ou l'accès non autorisé au réseau du Centre ;
- ✓ Vulnérabilités des systèmes d'exploitation et des routeurs, les systèmes d'exploitation et les routeurs du Centre n'ont pas de sécurité adéquate, donc ils peuvent présenter des vulnérabilités qui permettent aux attaquants d'accéder aux appareils ou de perturber leur fonctionnement ;
- ✓ Attaques de détection d'intrusion, les attaques de détection d'intrusion ciblent les systèmes de sécurité et les appareils de surveillance, visant à les contourner pour accéder au réseau ou aux données du Centre.

Ces risques potentiels liés à la vulnérabilité actuelle du réseau du Centre soulignent l'urgence d'une intervention appropriée. Ainsi, cette étude permettra d'explorer les mécanismes, les technologies et les meilleures pratiques pour concevoir, implémenter et gérer un système d'authentification efficace, adapté aux besoins spécifiques du Centre MURAZ, tout en garantissant la sécurité et la confidentialité des données.

1.4 Objectifs de l'Étude

1.4.1 Objectif principal

L'objectif central de l'étude consiste à concevoir, implémenter et gérer un système d'authentification efficace et adapté aux besoins spécifiques du Centre MURAZ. Cela englobe plusieurs aspects importants tels que :

- ✓ **Conception du système d'authentification**, la première étape est de concevoir un système d'authentification qui répond aux besoins uniques du Centre MURAZ. Cela nécessite une analyse approfondie des exigences en matière de sécurité, des flux de travail internes, des types d'utilisateurs et des ressources sensibles à protéger ;
- ✓ **Implémentation du système**, une fois le système conçu, il doit être mis en œuvre de manière robuste et fiable. Cela peut inclure la configuration des logiciels, des serveurs d'authentification, des bases de données utilisateur, des politiques de sécurité et des mécanismes d'authentification, tels que les mots de passe, la biométrie, la sécurité multi-facteurs (MFA), etc;
- ✓ **Gestion continue**, un système d'authentification nécessite une gestion continue pour garantir son efficacité et sa sécurité. Cela comprend la surveillance des activités d'authentification, la gestion des utilisateurs, la mise en place de politiques de sécurité, la maintenance des logiciels et des correctifs de sécurité, la révision des protocoles d'authentification, etc;
- ✓ **Adaptation aux besoins spécifiques**, le système d'authentification doit être adapté aux besoins spécifiques du Centre MURAZ, en prenant en compte les particularités de l'institut, telles que les types d'utilisateurs (chercheurs, personnel administratif, partenaires externes, etc.), les données sensibles stockées et les réglementations auxquelles il doit se conformer ;
- ✓ **Protection des données de recherche**, l'un des objectifs principaux est de garantir la protection des données de recherche, y compris les données

médicales et épidémiologiques, en veillant à ce qu'elles soient accessibles uniquement par des utilisateurs autorisés ;

- ✓ **Prévention des violations de sécurité**, le système d'authentification doit jouer un rôle clé dans la prévention des violations de sécurité en empêchant l'accès non autorisé aux systèmes, aux réseaux et aux données du Centre MURAZ ;
- ✓ **Conformité aux réglementations**, l'objectif est de garantir que le système d'authentification est conforme aux réglementations en matière de protection des données, de confidentialité et de sécurité de l'information, telles que le RGPD ou d'autres normes applicables ;
- ✓ **Facilitation de la recherche et de la collaboration**, le système d'authentification doit faciliter la recherche en permettant aux chercheurs d'accéder aux ressources et aux données nécessaires de manière sécurisée. Il doit également soutenir la collaboration avec d'autres institutions de recherche, en garantissant que l'accès aux données partagées soit contrôlé et sécurisé.

L'objectif principal de l'étude est de mettre en place un système d'authentification robuste, adapté aux besoins spécifiques du Centre MURAZ, afin de garantir la sécurité des données de recherche, la conformité aux réglementations, la prévention des violations de sécurité et la facilitation de la recherche et de la collaboration au sein de l'institut.

1.4.2 Objectifs secondaires

Les objectifs secondaires de cette étude visent à :

- ✓ **Améliorer l'efficacité opérationnelle**, le nouveau système d'authentification doit simplifier et accélérer les processus d'accès aux systèmes et aux données, ce qui améliorera l'efficacité des opérations au sein du Centre MURAZ ;

- ✓ **Réduire des erreurs et des risques**, un système d'authentification solide peut contribuer à réduire les erreurs humaines et les risques associés à l'accès non autorisé ou à la manipulation incorrecte de données médicales ;
- ✓ **Faciliter la gestion des comptes utilisateurs**, le système peut simplifier la gestion des comptes utilisateurs, y compris la création, la modification et la suppression de comptes, ainsi que la réinitialisation de mots de passe ;
- ✓ **Sensibiliser et à former des utilisateurs**, un objectif secondaire pourrait être de sensibiliser et de former les utilisateurs du Centre MURAZ à l'utilisation sécurisée du nouveau système d'authentification ;
- ✓ **Intégrer avec d'autres systèmes**, le système d'authentification peut être conçu pour s'intégrer de manière transparente avec d'autres systèmes et applications utilisés au Centre Muraz, ce qui simplifie l'accès aux ressources ;
- ✓ **Suivre des tendances de sécurité**, l'objectif peut être de rester à jour avec les dernières tendances en matière de sécurité informatique et d'adapter le système en conséquence pour répondre aux nouvelles menaces ;
- ✓ **Minimiser des coûts de support technique**, en simplifiant l'authentification et en réduisant les problèmes liés aux mots de passe oubliés ou aux comptes verrouillés, le Centre MURAZ peut réduire les coûts de support technique ;
- ✓ **Produire des rapports et audit de sécurité**, le système peut générer des rapports et des journaux d'audit pour permettre la surveillance de la sécurité et la vérification de la conformité aux politiques de sécurité.

1.5 Conclusion

Ce chapitre nous a permis de faire le point sur le contexte du projet en présentant notre structure d'accueil à travers son fonctionnement et ses activités. De plus il nous a permis de présenter le projet et de montrer le rôle du réseau IP au sein du Centre MURAZ. Dans le chapitre suivant, nous ferons une analyse des

besoins en sécurité en identifiant les besoins en sécurité et en faisant une évaluation des risques.

CHAPITRE 2 : ANALYSE DES BESOINS EN SECURITE

2.1. Introduction

Après avoir élaborer le contexte du projet, nous allons premièrement faire l'identification des besoins en sécurité. Cette partie permet de mettre en lumière les besoins spécifiques en matière de sécurité pour les données médicales et les services du Centre. Deuxièmement une évaluation des risques qui vise à identifier, évaluer, et atténuer les différences menaces et vulnérabilités qui peuvent nuire à la sécurité des informations du Centre. Et pour terminer, nous allons faire une brève conclusion pour résumer le chapitre.

2.2. Identification des Besoins de Sécurité

L'identification des besoins spécifiques en matière de sécurité pour les données médicales et les services du Centre est une étape essentielle pour assurer la protection adéquate de l'information sensible. Les besoins spécifiques en matière de sécurité pour les données médicales et les services du Centre sont :

- **Confidentialité**, garantir la confidentialité des données empêche une entité tierce (non autorisée, le plus souvent en état de fraude passive) de récupérer ces données et de les exploiter. Seuls les utilisateurs autorisés doivent être en mesure de prendre connaissance du contenu des données. Il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :
 - ✓ Cryptage des données, mettre en œuvre des mécanismes de cryptage pour protéger les données médicales lorsqu'elles sont stockées, transitent ou sont utilisées ;
 - ✓ Contrôles d'accès, établir des politiques de contrôle d'accès strictes pour garantir que seules les personnes autorisées ont accès aux données médicales du Centre ;

- **Intégrité**, le critère d'intégrité des ressources logiques (données médicales, traitements, transactions et services du Centre) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Il existe deux fonctions de sécurité qui permet de garder l'intégrité des données médicales et des services du Centre :
 - ✓ Gestion des versions, mettre en place des mécanismes pour suivre les modifications apportées aux données du Centre et assurer leur intégrité ;
 - ✓ Contrôles de modification, limiter l'accès et les droits de modification aux seules personnes autorisées ;
- **Disponibilité**, la disponibilité des données est relative à la période de temps pendant laquelle le service offert est opérationnel, ceci soit être en continu sans interruption, sans retard, ni dégradation. Pour garantir la disponibilité des services médicaux, il est important de mettre en place des mécanismes tels que :
 - ✓ Sauvegarde régulière, mettre en place des procédures de sauvegarde régulières pour garantir la disponibilité des données médicales et des services du Centre en cas de défaillance du système ;
 - ✓ Redondance des serveurs, établir une architecture informatique avec des systèmes redondants pour assurer la disponibilité continue des services du Centre ;
- **Non-répudiation**, c'est le fait de ne pas pouvoir nier ou rejeter qu'un événement (actions, transactions) a eu lieu. A ce critère de sécurité, peuvent être liées les notions suivantes :

- ✓ L'imputabilité qui est l'attribution d'une action (un événement) à une entité déterminée (ressources ou personnes).
 - ✓ La traçabilité permet de garder une trace numérique de tout événement (message électronique, transaction commerciale, transfert de données...).
 - ✓ L'audibilité définit la capacité d'un système à garantir la présence d'informations nécessaires à une analyse ultérieure d'un événement (courant ou exceptionnel) effectué dans le cadre de procédure de contrôle spécifique et d'audit.
- **Conformité aux réglementations**, il est important de se conformer aux réglementations en matière de protection des données médicales et des services du Centre :
- ✓ Documentation des politiques de sécurité, élaborer des politiques de sécurité conformes aux réglementations en vigueur, telles que la HIPAA (Health Insurance Portability and Accountability Act) aux États-Unis, le RGPD (Règlement Général sur la Protection des Données) en Europe, etc;
 - ✓ Audit de conformité, c'est une évaluation systématique des politiques, des procédures et des pratiques d'une organisation pour s'assurer qu'elles sont conformes aux normes et aux réglementations spécifiques. Dans le contexte de la sécurité des données médicales et des services du Centre, un audit de conformité vise à garantir que toutes les activités liées à la gestion de l'information médicale respectent les règles et les normes établies. Effectuer des audits réguliers pour s'assurer que les pratiques de sécurité sont en conformité avec les normes réglementaires ;

- **Sensibilisation à la sécurité**, fournir une formation régulière aux techniciens de laboratoires et aux autres personnels du Centre MURAZ sur les meilleures pratiques de sécurité et les menaces potentielles. Élaborer également des politiques de sécurité claires et s'assurer que tous les utilisateurs comprennent leurs responsabilités en matière de sécurité ;
- **Détection et réponse aux incidents**, mettre en place des systèmes de surveillance pour détecter les activités suspectes ou non autorisées. De plus, il faut avoir un plan d'intervention clair en cas de violation de sécurité ou d'incident.
- **Infrastructure de réseau sécurisée**, mettre en place des pare-feux et des systèmes de détection des intrusions pour protéger le réseau du Centre contre les attaques externes. Effectuer la mise à jour régulièrement des logiciels et des systèmes pour remédier aux vulnérabilités connues.
- **Gestion des identités**, surveiller et restreindre l'accès aux données médicales, en particulier les accès privilégiés. Utiliser également des méthodes d'authentification robustes pour garantir l'identité des utilisateurs.

En mettant en œuvre ces besoins spécifiques en matière de sécurité, le Centre peut renforcer sa posture de sécurité, minimiser les risques de violations de données et garantir la confidentialité, l'intégrité et la disponibilité des données médicales et des services.

2.3. Évaluation des Risques

L'évaluation des risques est une étape fondamentale dans la gestion de la sécurité des systèmes d'information, notamment dans le contexte des données médicales sensibles. Cette évaluation vise à identifier, évaluer et atténuer les différentes menaces et vulnérabilités qui peuvent nuire à la confidentialité, à l'intégrité et à la disponibilité des informations critiques du Centre MURAZ.

2.3.1. Identification des vulnérabilités

2.3.1.1. Vulnérabilités du réseau

Les vulnérabilités au niveau du réseau constituent une préoccupation cruciale pour la sécurité du système informatique du Centre MURAZ. Les vulnérabilités au niveau du réseau peuvent être :

- La présence de configurations réseau non sécurisées, telles que des ports ouverts inutiles, expose son infrastructure à des risques potentiels en offrant des points d'entrée vulnérables aux attaques ;
- L'utilisation de logiciels obsolètes ou non patchés constitue une faille de sécurité significative, car ces lacunes peuvent être exploitées par des cybercriminels pour accéder à son système ;
- Le manque de segmentation réseau, qui crée un environnement propice à la propagation rapide des attaques. En effet, une segmentation insuffisante permet aux cyberattaques de se propager rapidement à travers le réseau, compromettant davantage les systèmes.

Pour atténuer ces vulnérabilités, il est impératif de mettre en place des politiques de sécurité strictes, de maintenir constamment à jour ses logiciels et de mettre en œuvre une segmentation réseau efficace pour renforcer la résilience de son infrastructure face aux menaces potentielles.

2.3.1.2. Vulnérabilités des systèmes :

Les vulnérabilités au niveau des systèmes représentent une menace significative pour la sécurité des données médicales et les services du Centre, au niveau du système on peut avoir :

- Manque de mise à jour des systèmes d'exploitation, en réalité les systèmes d'exploitation constituent une cible majeure pour les attaquants, qui exploitent souvent des vulnérabilités connues. Le défaut de mise à jour

expose régulièrement le centre à des risques courus, car les correctifs de sécurité critiques ne sont pas appliqués. Les conséquences peuvent inclure l'exploitation de failles pour à des données sensibles, provoquer des interruptions de service ou exécuter des logiciels malveillants ;

- L'absence de contrôles d'accès appropriés aux bases de données , les bases de données médicales contiennent des informations sensibles sur les patients, telles que des données médicales, des diagnostics et des informations personnelles. L'absence de contrôles d'accès appropriés signifie qu'il peut être plus facile pour des personnes non autorisées d'obtenir un accès non autorisé à ces bases de données. Des mesures de sécurité inadéquates, telles qu'une gestion laxiste des identifiants et des droits d'accès, peuvent entraîner des fuites de données ou des manipulations malveillantes ;
- Le manque de chiffrement des données sensibles en transit , lorsque les données médicales circulent entre les différentes parties du système, notamment entre les dispositifs médicaux, les serveurs et les postes de travail, l'absence de chiffrement rend ces données vulnérables aux interceptions malveillantes. Le chiffrement des données en transit est crucial pour garantir la confidentialité des informations médicales et empêcher toute tentative d'interception ou de manipulation pendant la transmission.

Pour atténuer ces vulnérabilités, il est essentiel de mettre en place une politique de gestion des mises à jour rigoureuse, d'appliquer des contrôles d'accès stricts aux bases de données, d'utiliser des solutions de chiffrement robustes pour les données sensibles en transit, et de sensibiliser les utilisateurs aux bonnes pratiques de sécurité informatique. La protection des systèmes médicaux contre les vulnérabilités nécessite une approche holistique intégrant la technologie, les politiques et la formation des utilisateurs.

2.3.2. Identification des menaces

Une menace est une source de danger pour le système et se traduit par la présence d'une violation potentielle de la sécurité. Cela peut être une personne, une chose, un événement ou une idée qui constitue un danger à un patrimoine en termes de confidentialité, d'intégrité, de disponibilité et d'utilisation approuvée du système. La sécurité informatique doit faire face à une grande variété de menaces, elles peuvent être classées en deux catégories, externes et internes :

2.3.2.1. Menaces externes

Les menaces externes auxquelles le système du Centre MURAZ est exposé revêtent différentes formes, chacune représentant un risque potentiel pour la sécurité de ses services et ses données médicales sensibles. Comme menaces externe on peut avoir :

- Attaques de pirates informatiques visant à accéder aux données médicales sensibles, les attaques de pirates informatiques constituent une préoccupation majeure, car ces acteurs malveillants cherchent à infiltrer nos systèmes pour accéder à des informations confidentielles ;
- Malwares introduits par des e-mails malveillants ou des téléchargements non sécurisés, la menace de malwares persiste, avec des risques accumulés provenant d'e-mails malveillants ou de téléchargements non sécurisés, qui peuvent introduire des logiciels malveillants dans notre infrastructure ;
- Tentatives d'accès non autorisées aux systèmes depuis l'extérieur du réseau, il est impératif de rester vigilant face aux tentatives d'accès non autorisées depuis l'extérieur du réseau, où des individus recherchent à exploiter des vulnérabilités pour s'introduire dans nos systèmes.

En adoptant des mesures de sécurité robustes, nous pouvons réduire ces risques et renforcer la protection des services et des données médicales cruciales.

2.3.2.2. Menaces internes

Les menaces internes au système du Centre nécessitent une attention particulière, car elles peuvent émerger de diverses sources au sein même de notre structure d'accueil. Les menaces internes peuvent être :

- Accès non autorisé par des employés internes, les risques liés à un accès non autorisé par des employés internes sont inévitables, que ce soit intentionnellement par des individus malveillants ou par négligence due à une méconnaissance des protocoles de sécurité ;
- Erreurs humaines, les erreurs humaines telles que la configuration incorrecte des dispositifs réseau, représentent également une menace significative, pouvant nuire à la sécurité de l'infrastructure du Centre MURAZ ;
- Utilisation malveillante de privilèges d'accès internes, la possibilité d'une utilisation malveillante de privilèges d'accès internes ne doit pas être sous-estimée, car certains employés pourraient abuser de leurs autorisations pour des gains personnels ou malveillants.

En mettant en place des politiques de sécurité rigoureuses, une surveillance proactive et une sensibilisation continue au sein de notre structure d'accueil, nous pouvons atténuer ces risques internes et renforcer la robustesse du système de gestion des données du Centre.

2.3.3. Les risques

2.3.3.1. Matrice de Risques

La Matrice de Risques est un outil de gestion des risques largement utilisé dans de nombreux domaines, y compris la gestion de projet, la gestion d'entreprise, la gestion de la sécurité, et bien d'autres. Voici à quoi sert la matrice de risques :

- L'utilisation d'une matrice de risques constitue une étape fondamentale dans l'évaluation de la sécurité d'un réseau, permettant de mesurer la probabilité et l'impact associés à chaque combinaison de menace et de vulnérabilité. Cette approche systématique fournit une vision holistique des risques potentiels liés au Centre MURAZ qui pourraient être exposés. En fin de compte, l'utilisation d'une matrice de risques contribue à établir une base solide pour le développement de stratégies de sécurité proactives et adaptatives au sein du Centre ;
- Attribution de scores pour hiérarchiser les risques, en attribuant des scores appropriés à chaque menace-vulnérabilité, les professionnels de la sécurité peuvent hiérarchiser ces risques en fonction de leur gravité, facilitant ainsi une prise de décision éclairée pour orienter les efforts d'atténuation. Cette méthodologie permet de concentrer les ressources sur les risques les plus critiques, assurant ainsi une gestion efficace des vulnérabilités et une protection renforcée du réseau contre les menaces émergentes.

Il est à noter que cette matrice peut être adaptée en fonction des besoins spécifiques d'un projet ou d'une organisation. Par exemple, certains peuvent choisir d'ajouter des catégories supplémentaires pour affiner davantage l'évaluation des risques.

2.3.3.2. Hiérarchisation des Risques

La hiérarchisation des risques est une étape essentielle de la gestion des risques. Le processus de hiérarchisation des risques se déroule comme suit :

- Classement des risques en fonction des scores obtenus dans la matrice, cette étape implique le classement des risques en fonction des scores attribués dans la matrice d'évaluation, où la probabilité et l'impact de chaque combinaison menace-vulnérabilité sont soigneusement évalués. En procédant ainsi, le Centre peut distinguer clairement les risques les plus

préoccupants de ceux qui sont moins critiques. Ce classement offre une perspective stratégique, permettant aux responsables de la sécurité de se concentrer sur les vulnérabilités présentant les plus grands dangers. En mettant en lumière les risques les plus élevés, le Centre peut orienter ses ressources et ses efforts vers des mesures d'atténuation adaptées, renforçant ainsi la robustesse de ses défenses face aux menaces potentielles. La hiérarchisation des risques devient ainsi un outil décisionnel essentiel, guidant la mise en place de stratégies de sécurité proportionnées et efficaces pour protéger les données médicales sensibles du centre MURAZ ;

- Identification des risques ayant un impact élevé et une probabilité significative, cette identification précise repose sur l'évaluation systématique de chaque menace-vulnérabilité, où la probabilité d'occurrence et l'impact potentiel sont soigneusement évalués. En concentrant l'attention sur les risques associés à une probabilité significative et à un impact élevé, le Centre MURAZ peut cibler ses ressources et ses efforts vers les vulnérabilités les plus critiques. Ces risques identifiés deviennent ainsi la priorité absolue lors de la planification et de la mise en œuvre des mesures d'atténuation. Cette démarche permet au centre MURAZ de renforcer de manière proactive sa posture de sécurité en se concentrant sur les menaces les plus pressantes, assurant ainsi une protection optimale des données médicales sensibles et la préservation de l'intégrité de son infrastructure contre les risques les plus préoccupants.

La hiérarchisation des risques est une étape essentielle de la gestion des risques qui permet de concentrer les efforts sur les risques les plus critiques ou les plus urgents, afin de minimiser leur impact sur les objectifs ou les activités concernés.

2.3.4. Développement de Scénarios d'Attaque : Scénarios Réalistes

Élaboration de scénarios d'attaque adaptés aux menaces et vulnérabilités identifiées. Ces scénarios d'attaque peuvent être :

- **Scénario 1, le vol de données médicales,** il se déroule comme suit,
 - Un attaquant externe cible les systèmes informatiques du Centre MURAZ avec pour objectif le vol de données médicales sensibles. Après avoir effectué une analyse préliminaire, l'attaquant identifie une vulnérabilité dans le système de gestion des accès aux dossiers médicaux électroniques ;
 - L'attaquant exploite la vulnérabilité en utilisant des techniques d'ingénierie sociale pour obtenir les identifiants d'un employé. Une fois l'accès obtenu, il explore discrètement la base de données médicales, extrait des informations confidentielles telles que les dossiers médicaux, les diagnostics et les informations personnelles des patients. L'objectif est de nuire à la confidentialité des données médicales ;
 - L'objectif est d'évaluer la robustesse des contrôles d'accès, la résilience face aux attaques ciblées, et la capacité à détecter une activité anormale permettant de prévenir le vol de données médicales.

- **Scénario 2, l'interruption des Services Critiques,**
 - Un groupe d'attaquants lance une attaque par déni de service distribué (DDoS) visant à perturber les services critiques du Centre MURAZ. L'analyse des vulnérabilités met en évidence une exposition potentielle aux attaques DDoS en raison de certaines configurations réseau non sécurisées ;
 - Les attaquants exploitent ces vulnérabilités pour orchestrer une attaque DDoS, provoquant une saturation de la bande passante du centre MURAZ. Les services essentiels, tels que l'accès aux dossiers électroniques et les systèmes de communication, deviennent indisponibles, entraînant des retards significatifs dans la prestation des soins médicaux ;

- L'objectif est d'évaluer la résistance du Centre aux attaques DDoS, la capacité à atténuer l'impact sur la disponibilité des services critiques, et tester les procédures de reprise après incident.

Ces scénarios réalistes sont conçus pour mettre en lumière les vulnérabilités spécifiques du Centre MURAZ et pour tester de manière proactive sa préparation face à des attaques potentielles. Les résultats de ces simulations contribueront à renforcer la posture de sécurité du Centre en mettant en place des mesures adaptées pour atténuer ces menaces identifiées.

2.3.5. Évaluation de l'Impact Business :

L'évaluation sur l'impact business peut être un :

- **Impact sur les Opérations**, l'évaluation de l'impact sur les opérations suite à une violation de la sécurité dans le contexte médical est cruciale pour anticiper les conséquences financières et opérationnelles, ainsi que pour mesurer les impacts sur la confidentialité, l'intégrité et la disponibilité des données médicales ;
- **Impact Financier**, une violation de la sécurité peut entraîner des coûts significatifs pour le Centre MURAZ. Cela comprend les dépenses liées à la remise en état des systèmes compromis, la mise en place de mesures correctives, les enquêtes pour déterminer l'étendue de l'incident, les notifications légales obligatoires, et les éventuelles sanctions financières résultant de la non-conformité aux réglementations de protection des données ;
- **Impact Opérationnel**, une violation de la sécurité peut perturber gravement les opérations du Centre MURAZ. Les temps d'arrêt des systèmes critiques, la perte de productivité du personnel pendant la remise en état, et la nécessité de revoir les processus opérationnels pour renforcer la sécurité

sont autant de facteurs contribuant à l'impact opérationnel. De plus, la dégradation de la réputation du Centre peut entraîner une diminution de la fréquentation des patients et des partenaires ;

- **Impact sur la Confidentialité des Données du Centre**, la violation peut porter atteinte à la confidentialité des données médicales, ce qui peut entraîner une perte de confiance significative de la part des patients. Outre les implications financières liées aux enquêtes et aux notifications obligatoires, des actions en justice pourraient être engagées, aggravant ainsi l'impact financier global ;
- **Impact sur l'Intégrité des Données du Centre**, l'intégrité des données médicales peut être altérée, affectant la qualité des informations cliniques. Des données modifiées ou corrompues peuvent entraîner des erreurs de diagnostic, des traitements incorrects et des risques courus pour la sécurité des patients, nécessitant des efforts significatifs pour rétablir l'intégrité des données ;
- **Impact sur la Disponibilité des services du Centre**, une violation de la sécurité peut entraîner des interruptions dans l'accès aux données du Centre, impactant directement la disponibilité des services. Cela pourrait entraîner des retards dans la prestation des soins médicaux, notamment dans des situations d'urgence, avec des conséquences éventuellement graves pour les patients.

En résumé, l'évaluation de l'impact sur les opérations doit prendre en compte ces aspects financiers et opérationnels, tout en mettant en lumière les conséquences sur la confidentialité, l'intégrité et la disponibilité des services et des données médicales. Cela permettra au Centre MURAZ de mieux anticiper, prévenir et répondre aux violations de sécurité de manière proactive.

2.3.6. Détermination des Mesures de Contrôle

2.3.6.1. Mesures Actuelles

Ces mesures actuelles visent à réduire la probabilité d'occurrence des risques ainsi que leur impact sur les objectifs du projet. Comme mesures actuelles on peut avoir :

- L'évaluation de l'efficacité des contrôles de sécurité actuels, une évaluation approfondie des contrôles de sécurité existants permet de déterminer leur efficacité dans la protection des données médicales et des systèmes du centre. Cela implique une analyse des dispositifs de sécurité tels que les pare-feux, les systèmes de détection d'intrusion, les solutions antivirus, les politiques d'accès et les mécanismes de chiffrement. Des tests de pénétration et des simulations d'attaques peuvent être utilisés pour évaluer la résilience des contrôles face à des scénarios réalistes. Les résultats de ces évaluations permettent d'identifier les forces et les faiblesses des dispositifs de sécurité actuels ;
- L'identification des lacunes dans les dispositifs de protection existants, une fois l'efficacité des contrôles de sécurité réalisée, l'identification des lacunes devient essentielle. Cela implique de déterminer les points faibles dans la configuration des dispositifs de sécurité, les processus opérationnels, les politiques de sécurité et la sensibilisation du personnel. Les lacunes peuvent également résulter d'une mise en œuvre inadéquate des meilleures pratiques de sécurité ou d'une absence de mise à jour régulière des systèmes. Une attention particulière doit être portée aux zones où les risques potentiels sont les plus élevés, tels que l'accès aux données médicales sensibles et la protection du réseau.

2.3.6.2. Nouvelles Mesures de Contrôle

Pour renforcer davantage la sécurité du Centre MURAZ, de nouvelles mesures de contrôle peuvent être envisagées. Cela pourrait inclure l'implémentation de nouvelles mesures de sécurité tels que :

- Déploiement de Solutions de Prévention des Fuites de Données (DLP), l'introduction de solutions de prévention des fuites de données renforcera la capacité du Centre MURAZ à détecter et prévenir toute transmission non autorisée d'informations sensibles. Ces systèmes peuvent surveiller les flux de données et mettre en œuvre des politiques de sécurité pour bloquer ou alerter en cas de tentative de transfert non autorisé ;
- Implémentation de Contrôles d'Accès Biométriques, l'adoption de contrôles d'accès biométriques, tels que la reconnaissance faciale ou les empreintes numériques, renforcera l'authentification des utilisateurs, en particulier pour l'accès aux données médicales critiques. Cela ajoute une couche de sécurité supplémentaire en s'assurant que seules les personnes autorisées ont accès aux informations sensibles ;
- Renforcement des Politiques de Gestion des Identités et des Accès, renforcer les politiques de gestion des identités et des accès en mettant en place des procédures strictes de révocation des droits d'accès pour les anciens employés. Cela réduit le risque lié aux accès non autorisés et assure une gestion efficace des privilèges d'accès ;
- Adoption de Solutions de Surveillance Continue du Réseau, l'adoption de solutions de surveillance continue du réseau permettra une détection précoce des activités suspectes. Ces outils analysent en temps réel le trafic réseau, identifiant les comportements anormaux et facilitant une réponse immédiate en cas d'incident de sécurité ;

- Renforcement des Programmes de Sensibilisation du Personnel, intensification des programmes de formation sur la cybersécurité avec des sessions régulières pour informer le personnel des dernières menaces et des meilleures pratiques de sécurité. La sensibilisation continue est essentielle pour maintenir un niveau élevé de conscience et de vigilance au sein de la structure ;
- Mise à Jour de la Documentation des Politiques de Sécurité, la documentation des politiques de sécurité serait mise à jour pour refléter ces nouvelles mesures de contrôle. Cela garantit une compréhension claire des responsabilités individuelles, des procédures à suivre en cas d'incident, et des nouvelles directives de sécurité.

L'introduction de ces nouvelles mesures de contrôle vise à anticiper les menaces émergentes, à renforcer la résilience du Centre MURAZ face aux cyberattaques, et à maintenir un niveau élevé de protection des données médicales et des services critiques. En intégrant ces éléments dans la stratégie globale de sécurité, le Centre MURAZ peut améliorer proactivement sa posture de sécurité.

L'évaluation des risques liés à la vulnérabilité du réseau IP permet au Centre MURAZ de prise des décisions informées pour renforcer sa posture de sécurité et minimiser les risques potentiels associés à l'utilisation de ses systèmes informatiques.

2.4. Conclusion

Ce chapitre nous a été bénéfique car nous avons pu dans un premier temps, faire l'identification des besoins en sécurité. Cette partie qui a permis de mettre en lumière les besoins spécifiques en matière de sécurité pour les données médicales et les services du Centre. Dans un deuxième temps, nous avons fait une évaluation des risques. Dans le chapitre suivant, nous allons faire la sélection de la solution

d'authentification en faisant la revue des solutions disponibles et le choix de la solution d'authentification.

CHAPITRE 3 : SELECTION DE LA SOLUTION D'AUTHENTIFICATION

3.1. Introduction

Ce chapitre est rédigé en deux parties et fournit les clés de compréhension du projet. La première partie expose la revue des solutions disponibles en présentant les différentes solutions que nous avons trouvées et en faisant une étude comparative effectuée dans le but de trouver une solution répondant aux attentes du Centre MURAZ. Et, la seconde partie présente la sélection de la solution d'authentification la plus fiable et sécurisé.

3.2. Revue des Solutions Disponibles [5]

Bien qu'il ne s'agisse que d'une facette de la cybersécurité, l'authentification constitue la première ligne de défense. Elle sert à déterminer si un utilisateur est bien celui qu'il prétend être. L'authentification, à ne pas confondre avec l'étape qu'elle précède – à savoir l'autorisation – est simplement la mesure permettant de confirmer l'identification numérique, de sorte que les utilisateurs disposent du niveau d'autorisation nécessaire pour accéder à une tâche ou l'exécuter.

Il existe de nombreuses technologies d'authentification, des mots de passe aux empreintes digitales, pour confirmer l'identité d'un utilisateur avant de lui octroyer un accès. Leur utilisation permet d'ajouter une couche de protection et d'éviter les failles de sécurité telles que les violations de données. Cependant, c'est souvent la combinaison de différents types d'authentification qui permet de renforcer le système de sécurité contre les menaces éventuelles.

L'authentification empêche les utilisateurs non autorisés d'accéder aux bases de données, aux réseaux et autres ressources. Pour confirmer l'identité de l'utilisateur, ces types d'authentification font appel à des facteurs, une catégorie d'identifiants servant à la vérification. Voici quelques-unes de ces méthodes.

3.2.1 Authentification à facteur unique / primaire

Jusqu'à présent, la forme d'authentification la plus courante – à savoir l'authentification à facteur unique – est également considérée comme la moins sûre, en ce qu'elle ne nécessite qu'un seul facteur pour obtenir un accès complet au système. Ce facteur peut être un nom d'utilisateur avec un mot de passe, un code pin ou un autre code simple.

3.2.1.1 Avantages

Les avantages de l'authentification à facteur unique peuvent être :

- Simplicité, facile à mettre en place et à utiliser, ne nécessitant qu'un seul facteur d'authentification comme un mot de passe ;
- Coût, généralement moins coûteuse en termes de mise en œuvre et de maintenance ;
- Convivialité, facile pour les utilisateurs de s'en souvenir, ce qui peut améliorer l'expérience utilisateur.

3.2.1.2 Inconvénients

Comme inconvénients on a :

- Sécurité limitée, moins sécurisée comparée aux méthodes d'authentification multi-facteurs car elle repose uniquement sur un facteur (ex. : mot de passe) ;
- Vulnérabilité aux attaques, plus sujette aux attaques telles que le phishing ou le vol de mot de passe.

3.2.2 Authentification à deux facteurs (2FA)

L'authentification à deux facteurs renforce les efforts de sécurité grâce à un second facteur de vérification. Cette couche supplémentaire permet de vérifier de deux manières distinctes qu'un utilisateur est bien celui qu'il prétend être, ce qui complique considérablement les tentatives d'intrusion. Selon cette méthode, les

utilisateurs saisissent leurs informations d'authentification primaire (par exemple le nom d'utilisateur et le mot de passe susmentionnés) et doivent ensuite saisir une seconde information d'identification.

Le facteur secondaire est généralement plus difficile à violer, en ce qu'il fait souvent appel à une information à laquelle seul l'utilisateur autorisé a accès et qui est sans rapport avec le système en question. Parmi les facteurs secondaires possibles, citons : un mot de passe à usage unique provenant d'une application d'authentification, un numéro de téléphone ou un appareil pouvant recevoir une notification push ou un code SMS, ou encore un élément biométrique comme une empreinte digitale (Touch ID), un visage (Face ID) ou la reconnaissance vocale.

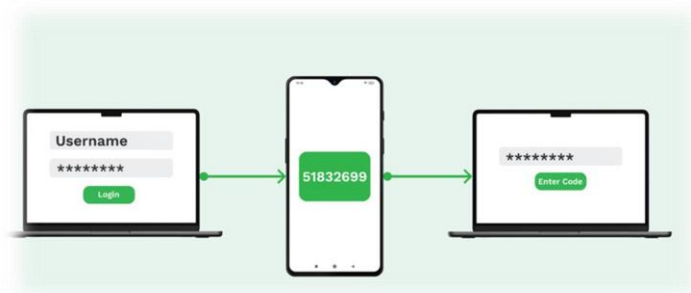


Figure 2: Principe de l'authentification à double facteurs (2FA) [5]

3.2.2.1 Avantages

Les avantages de l'authentications à double facteur sont :

- Sécurité renforcée, niveau de sécurité plus élevé en exigeant deux formes d'authentification (ex. : mot de passe et code à usage unique) ;
- Réduction des risques, l'authentification 2FA réduit considérablement les risques de compromission du système ou des ressources, étant donné qu'il est peu probable qu'un utilisateur non autorisé connaisse ou ait accès aux deux facteurs d'authentification.

De ce fait, bien qu'elle soit aujourd'hui très largement adoptée, l'authentification à deux facteurs entraîne quelques désagréments pour les

utilisateurs, ce qui constitue un obstacle à prendre en compte dans le cadre de la mise en œuvre.

3.2.2.2 Inconvénients

Ses inconvénients peuvent être :

- Complexité, peut être perçue comme plus complexe pour les utilisateurs en raison du besoin de fournir deux types d'informations ;
- Coût initial, peut nécessiter des coûts initiaux pour la mise en place de mécanismes 2FA.

3.2.3 Authentification unique (SSO)

Avec la technologie SSO, les utilisateurs ne doivent se connecter qu'à une seule application afin d'avoir accès à de nombreuses autres. Plus pratique pour les utilisateurs, cette méthode supprime l'obligation de conserver plusieurs ensembles d'informations d'identification et offre une expérience plus transparente pendant les sessions de travail.

Les entreprises peuvent la mettre en œuvre en désignant un domaine central (dans l'idéal, un système IAM), puis en créant des liens SSO sécurisés entre les ressources. Ce processus permet une authentification des utilisateurs surveillée par le domaine et, grâce à l'authentification unique, elle est en mesure de garantir que lorsque les utilisateurs autorisés mettent fin à leur session, ils se déconnectent correctement de toutes les ressources et applications liées.

3.2.3.1 Avantages

Quelques avantages de SSO :

- Facilité d'utilisation, simplifie l'accès à plusieurs services avec un seul ensemble d'identifiants, améliorant la convivialité ;

- Productivité : Réduit la nécessité de se reconnecter fréquemment, ce qui peut augmenter la productivité.

3.2.3.2 Inconvénients

L'authentification unique nécessite une :

- Sécurité relative, moins sécurisée comparée à certaines méthodes 2FA, car l'accès compromis à un service peut potentiellement donner accès à d'autres ;
- Dépendance au fournisseur, souvent dépendante d'un fournisseur SSO, introduisant une dépendance externe.

3.2.4 Authentification multifactorielle (MFA)

L'authentification multifactorielle est une méthode d'une grande fiabilité, car elle utilise davantage de facteurs non pertinents pour le système afin de légitimer les utilisateurs. À l'instar de la méthode 2FA, l'authentification MFA fait appel à des facteurs tels que des données biométriques, la confirmation axée sur l'appareil, des mots de passe supplémentaires, voire des informations basées sur le lieu ou le comportement (par exemple, un modèle de frappe ou une vitesse de frappe), pour confirmer l'identité de l'utilisateur. Cependant, la différence entre ces deux méthodes réside dans le fait que si l'authentification 2FA n'utilise dans tous les cas que deux facteurs, l'authentification MFA peut en utiliser deux ou trois, avec la possibilité de varier entre les sessions, ce qui ajoute un élément insaisissable pour les utilisateurs non autorisés.

3.2.4.1 Avantages

Les avantages de la MFA sont :

- Sécurité maximale, offre le plus haut niveau de sécurité en utilisant trois ou plus de trois facteurs d'authentification ;
- Adaptabilité, plus de flexibilité dans le choix des facteurs, tels que biométrie, carte à puce, etc.

3.2.4.2 Inconvénients

Les inconvénients de la MFA :

- Complexité et Coût : Plus complexe à mettre en œuvre et peut nécessiter des coûts supplémentaires.
- Gestion des Utilisateurs : Peut nécessiter une gestion plus poussée des utilisateurs et de leurs appareils.

3.2.5 Les protocoles d'authentification les plus courants

Les protocoles d'authentification sont les règles d'interaction et de vérification désignées que les points d'entrée (ordinateurs portables, ordinateurs de bureau, téléphones, serveurs, etc.) ou les systèmes utilisent pour communiquer. Il existe autant d'applications distinctes auxquelles les utilisateurs doivent accéder que de normes et de protocoles. Le choix du bon protocole d'authentification pour votre entreprise est essentiel pour garantir la sécurité des opérations et la compatibilité des utilisations. Voici quelques-uns des protocoles d'authentification les plus couramment utilisés.

3.2.5.1 Protocole d'authentification par mot de passe (PAP)

Bien que courant, le protocole PAP est le moins sûr pour la validation des utilisateurs, principalement en raison de son manque de chiffrement. Il s'agit essentiellement d'un processus de connexion de routine qui requiert une combinaison de nom d'utilisateur et de mot de passe pour accéder à un système donné, validant ainsi les informations d'identification fournies. Il est désormais le plus souvent utilisé comme dernière option pour communiquer entre un serveur et un ordinateur de bureau ou un appareil distant.

3.2.5.2 Protocole d'authentification par défi-réponse (CHAP)

Le protocole CHAP est un protocole de vérification d'identité permettant de vérifier l'identité d'un utilisateur sur un réseau donné, à l'aide d'une norme de chiffrement supérieure faisant appel à un échange tripartite d'un « secret ». Tout d'abord, le routeur local envoie un « défi » à l'hôte distant, lequel renvoie une réponse avec une fonction de hachage MD5. Le routeur compare la réponse renvoyée à la réponse attendue (valeur de hachage) et, selon qu'il détermine ou non une correspondance, il établit une connexion authentifiée – appelée « poignée de main » – ou refuse l'accès. Il est intrinsèquement plus sûr que le protocole PAP, car le routeur peut envoyer un défi à tout moment d'une session, tandis que le protocole PAP n'entre en jeu que lors de l'approbation d'authentification initiale.

3.2.5.3 Protocole d'authentification extensible (EAP)

Ce protocole prend en charge de nombreux types d'authentification, des mots de passe à usage unique aux cartes à puce. Lorsqu'il est utilisé dans le cadre des communications sans fil, le protocole EAP représente le niveau de sécurité le plus élevé, en ce qu'il permet à un point d'accès donné et à un appareil distant d'effectuer une authentification mutuelle avec chiffrement intégré. Il connecte les utilisateurs au point d'accès qui sollicite des informations d'identification, il confirme l'identité par l'intermédiaire d'un serveur d'authentification et demande ensuite une autre forme d'identification de l'utilisateur en vue d'une nouvelle confirmation par le serveur, après quoi il achève le processus avec tous les messages transmis sous une forme chiffrée.

3.2.6 Tableau de comparaison des solutions [3]

Tableau 1:Tableau comparatif des solutions

Caractéristiques	Authentification à facteur unique	Authentification à double facteurs (2FA)	Authentification Unique (SSO)	Authentification Multifactorielle (MFA)
Principe	✓	✓	✗ Un seul ensemble d'identifiants fourni pour accéder à plusieurs services ou applications.	✓
Sécurité	✗ Modérée en raison de la dépendance sur un seul facteur.	✓	✓	✓
Convivialité	✓	✓	✓	✗ Peut nécessiter des étapes supplémentaires, mais cela dépend du type de facteurs utilisés.
Coût	✓	✓	✗ Peut-être coûteux en raison de la mise en place d'une	✓

			infrastructure centralisée.	
Fiabilité	✗ Modérée, car la sécurité repose principalement sur un seul facteur.	✓.	✓	✓
Récupération en cas d'oubli	✓	✓	✓	✓
Exemples	Mot de passe uniquement.	Mot de passe + Code à usage unique.	Connexion unique à plusieurs services avec un seul ensemble d'identifiants.	Mot de passe + Empreinte digitale + Code à usage unique.
Utilisation courante	✓	✓	✓	✓

Les symboles "✓" indiquent que la caractéristique est généralement présente ou réussie pour la méthode respective, tandis que le symbole "✗" indique l'absence ou des limitations.

3.3.Choix de la Solution d'Authentification

Nous avons plusieurs méthodes d'authentification à notre disponibilité. Le Centre MURAZ préfère une méthode d'authentification sécurisée et fiable. Ce qui exclut l'utilisation de l'authentification à facteur unique. L'authentification multifactorielle utilise plusieurs facteurs d'authentification ce qui rend parfois le processus plus complexe pour les utilisateurs. Certains peuvent trouver fastidieux

de devoir fournir plusieurs types d'informations ou d'effectuer plusieurs étapes pour se connecter alors que le Centre préfère un système d'authentification convivial. Maintenant, voyons laquelle des deux méthodes (**2FA** et **SSO**) est la meilleure. Le tableau suivant montre la comparaison entre les deux types d'authentifications.

Tableau 2: Comparaison entre 2FA et SSO [3]

Caractéristiques	Authentification à double facteurs (2FA)	Authentification unique (SSO)
Flexibilité	Plus flexible dans le choix des facteurs d'authentification (SMS, application mobile, token, etc.).	Généralement moins flexible en termes de types de facteurs d'authentification, car il se repose sur un mécanisme unique.
Sensibilité des données	Bien adapté aux environnements traitant des données très sensibles, car il offre un niveau de sécurité élevé.	Convient pour les environnements où la commodité est primordiale et où la sensibilité des données peut varier d'un service à l'autre.

Gestion des sessions	Généralement moins complexe en termes de gestion des sessions, car chaque service peut avoir son propre mécanisme de session.	La gestion des sessions doit être soigneusement gérée pour assurer la déconnexion appropriée après l'utilisation d'un service.
Exemples d'utilisation courante	Accès à des applications professionnelles, données sensibles, systèmes informatiques critiques.	Environnements de bureau, accès à des services cloud, applications d'entreprise.
Dépendance envers le fournisseur	Non	Oui

Il est important de noter que le choix entre L'authentification à double facteurs (2FA) et l'authentification unique (SSO) dépend des besoins spécifiques de sécurité, de dépendance envers le fournisseur et d'infrastructure de chaque organisation. Nous envisageons l'utilisation de l'authentification à double facteurs (2FA) comme système d'authentification sur certains critères :

- Le Centre MURAZ traite souvent des données hautement sensibles, notamment des informations médicales confidentielles et des résultats d'essais cliniques. L'ajout d'un deuxième facteur d'authentification renforce la protection de ces données contre tout accès non autorisé.
- Dépendance envers le Fournisseur : Dépend de la mise en œuvre spécifique et peut être mis en place de manière indépendante.

Nous venons de recenser des points touchants des exemples de solutions en évoquant leurs fonctionnements d'abord, ensuite nous avons mis en évidence un tableau comparatif en fonction de nos besoins et cela nous a permis de choisir le système d'authentification à double facteurs (2FA).

3.4. Conclusion

Ce chapitre vient de recenser des points touchants des exemples de solutions en évoquant leurs caractéristiques d'abord, ensuite elle a mis en évidence un tableau comparatif en fonction de nos besoins et cela nous a permis de choisir la méthode d'authentification. Le prochain chapitre donne une étude approfondie afin de faciliter sa mise en œuvre.

CHAPITRE 4 : CONCEPTION DU SYSTHEME D'AUTHENTIFICATION

4.1 Introduction

Dans ce chapitre, nous allons faire une conception détaillée du système d'authentification à double facteurs. En effet, nous allons étudier le principe de fonctionnement du système d'authentification à double facteurs tout en présentant son architecture, les protocoles et technologies utilisés. Cela nous permettra d'avoir une maîtrise du système d'authentification choisi.

4.2 Architecture du Système d'Authentification

La conception d'un système d'authentification à double facteur (2FA) implique l'utilisation de deux méthodes distinctes pour vérifier l'identité d'un utilisateur. Voici un schéma détaillé de l'architecture d'un système d'authentification 2FA, en intégrant les composantes critiques.

4.2.1 Composantes principales

Comme composantes principales on a :

➤ Utilisateur

Dans le contexte de l'authentification, l'utilisateur constitue l'une des composantes principales du processus. L'identification de l'utilisateur est essentielle pour établir son identité au sein du système. Cela implique généralement la fourniture d'un nom d'utilisateur et d'un mot de passe comme facteurs de connaissance. L'utilisateur est responsable de démontrer son autorisation à accéder au système en fournissant des informations d'identification valides. Dans des scénarios plus avancés d'authentification à deux facteurs (2FA) ou multi-facteurs (MFA), l'utilisateur pourrait également interagir avec des dispositifs physiques, des applications d'authentification, ou des méthodes biométriques pour renforcer la vérification de son identité. La gestion sécurisée des informations d'identification de l'utilisateur est cruciale pour prévenir les accès non autorisés ;

➤ **Serveur d'Authentification**

Le serveur d'authentification est une composante clé du processus d'authentification. Il joue un rôle central dans la vérification de l'identité des utilisateurs tentant d'accéder au système. Le serveur d'authentification reçoit les informations d'identification fournies par l'utilisateur, telles que le nom d'utilisateur et le mot de passe. Il compare ensuite ces données avec celles stockées de manière sécurisée dans sa base de données pour déterminer la validité de l'authentification. Dans des systèmes avancés, le serveur peut également interagir avec des composants de deuxième facteur, comme des applications d'authentification mobiles ou des clés de sécurité physiques, pour renforcer la sécurité. La robustesse de la sécurité du système dépend en grande partie de la conception et de la gestion sécurisée du serveur d'authentification, qui doit résister aux tentatives d'accès non autorisées et garantir la confidentialité des informations stockées ;

➤ **Base de Données d'Utilisateur**

La base de données d'utilisateur est une composante fondamentale du processus d'authentification. Elle stocke de manière sécurisée les informations d'identification associées aux utilisateurs autorisés. Ces données peuvent inclure des noms d'utilisateur, des mots de passe hachés, des clés de sécurité, des paramètres d'authentification à deux facteurs (2FA), et d'autres informations pertinentes. Lorsque l'utilisateur fournit ses informations d'identification, le serveur d'authentification consulte la base de données d'utilisateur pour vérifier la validité des données. La sécurisation adéquate de la base de données est cruciale pour protéger les informations sensibles contre les accès non autorisés. Des techniques telles que le hachage des mots de passe et le salage sont souvent utilisées pour renforcer la sécurité des données stockées dans la base de données d'utilisateur ;

➤ **Générateur de Codes Temporels (TOTP)**

Le générateur de codes temporels (TOTP) est une composante qui participe à la mise en œuvre de l'authentification à deux facteurs (2FA). Le TOTP utilise un algorithme qui génère des codes à usage unique basés sur le temps. Ce code change périodiquement, souvent toutes les 30 secondes, ce qui renforce la sécurité du processus d'authentification. L'utilisateur possède généralement un dispositif, tel qu'une application mobile dédiée, qui génère ces codes TOTP. Lors de l'authentification, l'utilisateur fournit le code TOTP actuel en plus de son mot de passe. Cette composante ajoute une couche de sécurité supplémentaire, nécessitant à la fois quelque chose que l'utilisateur sait (le mot de passe) et quelque chose qu'il possède (le dispositif générant le code TOTP), renforçant ainsi la vérification d'identité ;

➤ **Mécanisme de Livraison de Codes (SMS, Email, Application Authentificateur)**

Le mécanisme de livraison de codes est une composante qui facilite la distribution sécurisée des codes d'authentification à deux facteurs (2FA) aux utilisateurs. Ce mécanisme peut prendre différentes formes, telles que l'envoi de codes par SMS, courriel, ou applications dédiées. L'utilisateur reçoit le code sur un dispositif sécurisé, généralement son téléphone mobile, en complément de son mot de passe. Le mécanisme de livraison de codes est essentiel pour assurer que le deuxième facteur d'authentification parvienne à l'utilisateur de manière fiable et sécurisée. La sécurité de ce processus est cruciale pour éviter toute interception ou accès non autorisé aux codes d'authentification, garantissant ainsi l'intégrité du processus d'authentification à deux facteurs.

4.2.2 Processus d'Authentification

L'authentification fonctionne comme suit :

- L'utilisateur fournit son nom d'utilisateur et son mot de passe au serveur d'authentification ;
- Le serveur d'authentification vérifie ces informations en les comparant à celles stockées dans la base de données d'utilisateur ;
- Si les informations d'identification traditionnelles sont correctes, le serveur génère un défi 2FA ;
- Le serveur envoie le défi à l'utilisateur ;
- L'utilisateur utilise son dispositif 2FA (comme une application authenticatrice mobile) pour générer un code unique basé sur le défi et la clé secrète partagée ;
- L'utilisateur soumet ce code au serveur d'authentification ;
- Le serveur d'authentification vérifie le code 2FA en le comparant à celui attendu (calculé également à partir du défi et de la clé secrète) ;
- Si la correspondance est réussie, le serveur autorise l'accès, confirmant ainsi l'identité de l'utilisateur.

4.2.3 Architecture du système d'authentification à double facteurs

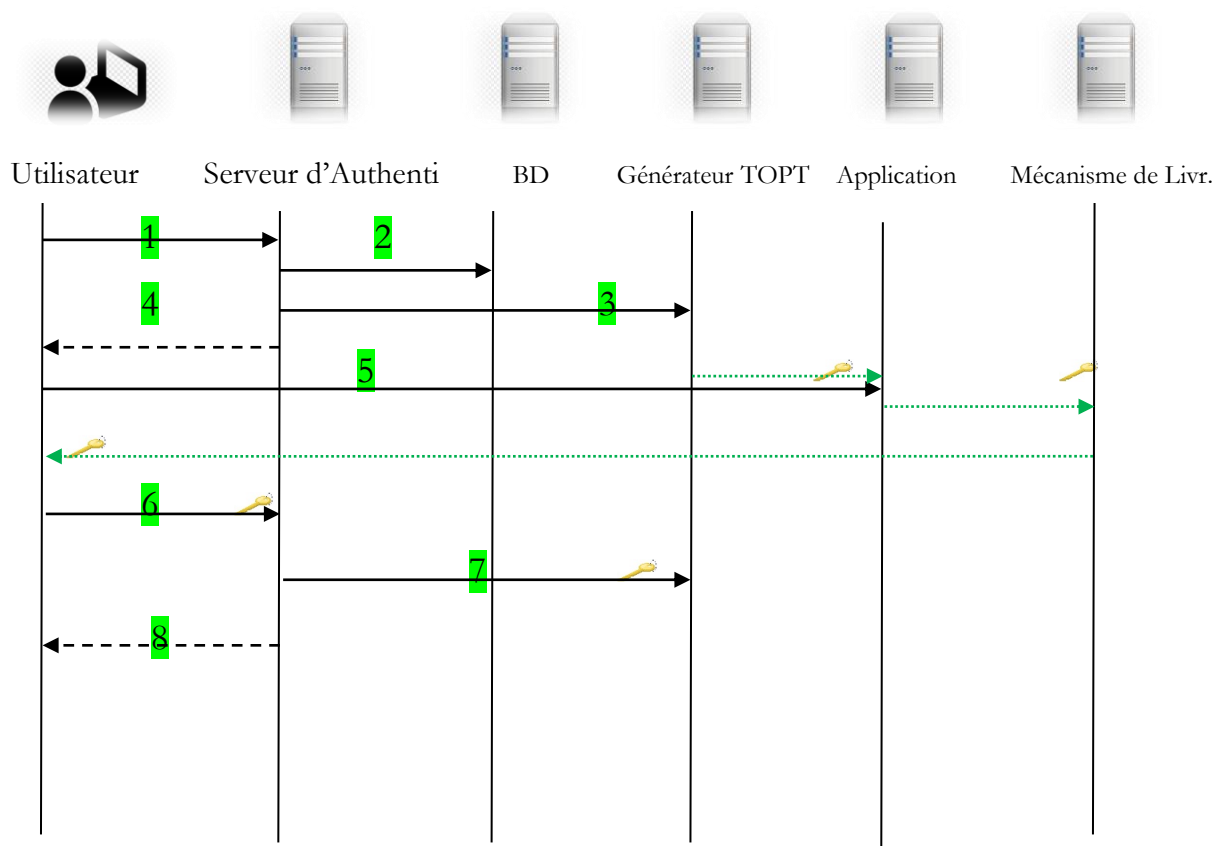


Figure 3: Architecture du système 2FA [12]

4.3 Protocoles et Technologies Utilisés

L'implémentation de l'authentification à deux facteurs (2FA) implique l'utilisation de protocoles et de technologies spécifiques pour renforcer la sécurité du processus d'authentification. Voici une description des protocoles et technologies couramment utilisés dans le contexte de l'authentification 2FA :

4.3.1 Time-based One-Time Password (TOTP)

TOTP est un protocole qui génère des codes à usage unique basés sur le temps. Il repose sur l'utilisation d'une clé secrète partagée entre le serveur

d'authentification et l'application 2FA de l'utilisateur. La clé secrète et l'horodatage actuel sont utilisés pour générer un code temporaire qui change à intervalles réguliers.

4.3.1.1 Fonctionnement de TOTP

Voici comment fonctionne TOTP :

- Configuration initiale, l'utilisateur et le serveur partagent un secret commun, généralement échangé lors de l'enregistrement du dispositif d'authentification (comme une application mobile) ;
- Génération du code,
 - Le code TOTP est généré à partir d'un algorithme cryptographique qui prend en compte le temps et le secret partagé.
 - Un compteur de temps, généralement en secondes, est utilisé comme input dans cet algorithme ;
- Synchronisation temporelle, l'horloge du dispositif d'authentification (généralement un téléphone) et du serveur doivent être synchronisées pour garantir que le code généré soit valide des deux côtés ;
- Période de validité, un paramètre important est la "période" ou "interval", indiquant la durée de validité d'un code TOTP.

Par exemple, si la période est définie à 30 secondes, un nouveau code TOTP est généré toutes les 30 secondes ;
- Saisie du Code TOTP, l'utilisateur saisit le code TOTP actuel dans l'interface d'authentification ;
- Validation, le serveur vérifie la validité du code TOTP en générant un code basé sur le secret partagé et le temps actuel, puis compare le résultat avec le code saisi par l'utilisateur ;

- Renouvellement périodique, le code TOTP change automatiquement à intervalles réguliers, améliorant la sécurité en cas de vol ou d'interception du code.

4.3.1.2 Formule de génération TOTP

La formule utilisée par TOTP est:

$$\text{TOTP} = \text{HOTP}(K, T)$$

Où :

- T est le compteur de temps ou un instantané de temps divisé par la période.
- K est le secret partagé (la clé).

4.3.1.3 Avantages de TOTP

Comme avantage on a :

- Dynamique : Les codes changent fréquemment, ce qui renforce la sécurité.
- Facile à Implanter : Les algorithmes TOTP sont largement pris en charge par des applications d'authentification standard.

🔗 Google Authenticator, Microsoft Authenticator et d'autres applications similaires utilisent l'algorithme TOTP pour générer des codes à usage unique.

4.3.2 HMAC-Based One-Time Password (HOTP)

HOTP est similaire à TOTP, mais au lieu de dépendre du temps, il utilise un compteur pour générer des codes à usage unique. Le compteur est incrémenté après chaque utilisation du code.

4.3.2.1 Fonctionnement de HOTP

Voici comment fonctionne HOTP :

- Configuration initiale, l'utilisateur et le serveur partagent un secret commun, généralement échangé lors de l'enregistrement du dispositif d'authentification ;
- Génération du code,
- Le code HOTP est généré à partir d'un algorithme de HMAC (Hash-based Message Authentication Code) qui utilise le secret partagé et un compteur comme inputs.
- Le compteur est incrémenté chaque fois qu'un nouveau code est généré ;
 - Saisie du code HOTP, l'utilisateur saisit le code HOTP actuel dans l'interface d'authentification ;
 - Validation, le serveur vérifie la validité du code HOTP en générant un code basé sur le secret partagé et le compteur actuel, puis compare le résultat avec le code saisi par l'utilisateur ;
 - Renouvellement manuel du Compteur, le compteur est généralement incrémenté manuellement côté serveur et par le dispositif d'authentification après chaque utilisation réussie.

4.3.2.2 Formule de Génération HOTP

La formule utilisée par HOTP est :

$$\text{HOTP}(K,C)=\text{Truncate}(\text{HMAC}(K,C))$$

Où :

- K est le secret partagé (la clé).
- C est le compteur.

4.3.2.3 Avantages de HOTP

Les avantages de HOTP sont :

- Indépendant du Temps : Contrairement à TOTP, HOTP ne dépend pas du temps, ce qui le rend moins susceptible aux problèmes de synchronisation temporelle.
- Facile à Implanter : Les algorithmes HMAC sont bien établis et pris en charge par de nombreuses bibliothèques cryptographiques.

4.3.2.4 Inconvénients de HOTP

Nécessite une Synchronisation Manuelle : Le compteur doit être synchronisé manuellement entre le dispositif d'authentification et le serveur, ce qui peut être moins pratique.

✎ Bien que HOTP ne soit pas aussi largement utilisé que TOTP dans les applications d'authentification, il reste une option valable, en particulier lorsque la synchronisation temporelle pose des défis.

4.3.3 Universal 2nd Factor (U2F)

Universal 2nd Factor (U2F) est une norme d'authentification ouverte qui vise à simplifier et renforcer les mécanismes de sécurité en introduisant une méthode d'authentification matérielle basée sur des clés de sécurité physique. Le U2F est conçu pour améliorer la sécurité tout en fournissant une expérience utilisateur fluide. Il a été développé par l'Alliance FIDO (Fast Identity Online) et est largement utilisé dans des applications en ligne pour renforcer la sécurité des comptes.

4.3.3.1 Caractéristiques principales de U2F

Les caractéristiques principales de U2F sont :

❖ Authentification Matérielle

- U2F utilise des clés de sécurité matérielles, telles que des clés USB ou des dispositifs NFC (Near Field Communication), pour renforcer l'authentification,
- Ces clés de sécurité stockent des certificats cryptographiques et génèrent des paires de clés publiques/privées ;

❖ Sans Mot de Passe

- U2F élimine la nécessité de saisir manuellement des mots de passe lors de l'authentification,
- L'utilisateur connecte simplement la clé de sécurité et appuie sur un bouton pour valider son identité ;

❖ Interopérabilité

- U2F est conçu pour être une norme ouverte et interopérable entre différents fournisseurs et applications,
- Il est pris en charge par divers services en ligne et navigateurs ;

❖ Protection contre le Phishing

- En raison de l'interaction physique requise (appuyer sur un bouton), U2F aide à prévenir les attaques de phishing, car l'authentification nécessite une action physique de l'utilisateur ;

❖ Protection contre les Attaques de MitM (Man-in-the-Middle)

- Les clés U2F intègrent des mécanismes de sécurité pour détecter et se protéger contre les attaques de type Man-in-the-Middle ;

4.3.3.2 Processus d'Authentification avec U2F

L'authentification avec U2F se déroule comme suit :

- ❖ L'utilisateur insère sa clé U2F dans un port USB ou active le mode NFC sur son appareil ;
- ❖ L'application ou le site web sollicite l'authentification U2F ;
- ❖ L'utilisateur appuie sur le bouton de la clé U2F pour confirmer son identité ;
- ❖ La clé U2F génère une signature cryptographique basée sur le contexte d'authentification ;
- ❖ La signature est envoyée au serveur d'authentification pour validation ;
- ❖ Si la signature est validée, l'utilisateur est authentifié avec succès.



Figure 4: Une clé USB U2F [6]

4.3.3.3 Avantages de U2F

Voici les avantages de U2F :

- Sécurité améliorée, l'utilisation de clés de sécurité matérielles renforce la sécurité de l'authentification,
- Utilisation simple, l'expérience utilisateur est simplifiée avec une authentification sans mot de passe ;

✎ Les navigateurs tels que Chrome, Firefox et Edge prennent en charge U2F. De nombreuses applications en ligne, y compris des services tels que Google,

Facebook et Dropbox, offrent la prise en charge de U2F pour renforcer la sécurité des comptes.

4.3.4 WebAuthn (Web Authentication)

WebAuthn (Web Authentication) est une spécification du World Wide Web Consortium (W3C) qui définit une norme d'authentification Web moderne et sécurisée. Elle vise à remplacer les méthodes d'authentification traditionnelles, en offrant une expérience utilisateur sans mot de passe, tout en renforçant la sécurité. WebAuthn prend en charge divers facteurs d'authentification, tels que les clés de sécurité, les empreintes digitales et les appareils mobiles.

4.3.4.1 Caractéristiques principales de WebAuthn

Les caractéristiques principales de WebAuthn sont :

- Authentification sans mot de passe, WebAuthn permet une authentification sans mot de passe en utilisant des mécanismes cryptographiques modernes ;
- Support de plusieurs facteurs d'authentification, WebAuthn prend en charge une variété de facteurs d'authentification, y compris les clés de sécurité, les empreintes digitales, les appareils mobiles et d'autres dispositifs biométriques ;
- Interopérabilité, comme U2F, WebAuthn est conçu pour être une norme ouverte et interopérable entre différents navigateurs et plates-formes ;
- Résistance aux attaques, WebAuthn intègre des mécanismes de sécurité pour résister aux attaques telles que le phishing et le détournement de session ;
- Confidentialité, les informations d'identification ne sont pas stockées sur le serveur, améliorant la confidentialité des utilisateurs.

4.3.4.2 Processus d'Authentification avec WebAuthn

Le processus général de l'authentification avec WebAuthn :

- Enregistrement, l'utilisateur enregistre un périphérique d'authentification (clé de sécurité, appareil biométrique, etc.) auprès du service en ligne ;
- Création d'attestation, le périphérique génère une paire de clés cryptographiques (publique/privée) et crée une attestation signée par la clé privée ;
- Stockage de l'attestation sur le serveur, l'attestation, accompagnée de la clé publique, est stockée sur le serveur ;
- Authentification, lors de l'authentification, le serveur demande à l'utilisateur de prouver sa possession du périphérique d'authentification ;
- Génération de la signature, le périphérique génère une signature basée sur la demande d'authentification ;
- Validation de la signature, le serveur valide la signature en utilisant la clé publique préalablement enregistrée ;
- Authentification réussie, si la signature est valide, l'authentification est réussie.

4.3.4.3 Avantages de WebAuthn

Comme avantages on a :

- Authentification sans mot de passe, élimination de la dépendance aux mots de passe ;
- Sécurité améliorée, utilisation de mécanismes cryptographiques modernes ;
- Polyvalence des facteurs d'authentification, support de divers facteurs d'authentification.

WebAuthn est de plus en plus adopté par les navigateurs et les services en ligne en tant que standard pour l'authentification sans mot de passe.

4.3.4.4 Inconvénients de WebAuthn

Comme inconvénients on a :

- Compatibilité limitée, bien que de nombreux navigateurs prennent désormais en charge WebAuthn, il peut y avoir des problèmes de compatibilité avec certains navigateurs plus anciens ou moins populaires. Cela peut limiter l'adoption de WebAuthn dans certains environnements ;
- Dépendance technologique, comme toute technologie de sécurité, WebAuthn est soumis à des failles potentielles. Si une vulnérabilité est découverte dans le protocole ou dans une implémentation particulière, cela pourrait compromettre la sécurité des systèmes qui utilisent WebAuthn ;
- Complexité pour les utilisateurs, bien que WebAuthn vise à simplifier l'expérience de connexion en éliminant les mots de passe, il peut introduire une certaine complexité pour les utilisateurs qui ne sont pas familiers avec les méthodes d'authentification alternatives telles que les clés de sécurité ou la biométrie.

4.3.5 SMS (Short Message Service)

L'utilisation de SMS (Short Message Service) dans le contexte de l'authentification est souvent associée à une méthode de vérification à deux facteurs (2FA) où un code de vérification est envoyé à l'utilisateur par SMS pour renforcer la sécurité de l'accès à un compte ou à une application. Cependant, il est important de noter que l'authentification par SMS présente certaines vulnérabilités et est de moins en moins recommandée en raison de problèmes potentiels de sécurité.

4.3.5.1 Processus d'Authentification par SMS

Le processus d'authentification par SMS se déroule comme suit :

- Demande d'identification, l'utilisateur entre son nom d'utilisateur et son mot de passe sur l'interface d'authentification ;
- Vérification des identifiants, le système vérifie les identifiants fournis par l'utilisateur ;
- Envoi du code par SMS, si les identifiants sont valides, un code de vérification unique est généré par le serveur d'authentification ;
- Envoi du code à l'utilisateur, le code est envoyé à l'utilisateur via un message SMS sur son numéro de téléphone mobile enregistré ;
- Saisie du code, l'utilisateur reçoit le code par SMS et le saisit dans l'interface d'authentification pour compléter le processus ;
- Validation du code, le système vérifie la correspondance du code saisi avec celui généré par le serveur ;
- Authentification réussie, si le code est valide, l'utilisateur est authentifié avec succès et accède au compte ou à l'application.

4.3.5.2 Avantage de l'Authentification par SMS

Comme avantage, le processus est relativement simple pour les utilisateurs, ne nécessitant qu'un téléphone mobile pour recevoir les codes.

4.3.5.3 Inconvénients et Limitations

Les limites de l'authentification par sms peuvent être :

- Vulnérabilité au Phishing, les attaques de phishing peuvent intercepter les codes envoyés par SMS ;

- Sim Swapping, les attaques de remplacement de carte SIM peuvent permettre à un attaquant de rediriger les messages SMS vers leur propre appareil ;
- Coût, dans certaines régions, l'envoi de SMS peut entraîner des coûts ;
- Fiabilité du réseau, les retards ou l'absence de réception des SMS peuvent poser problème.

✎ L'authentification par SMS est de plus en plus remplacée par des méthodes plus sécurisées telles que l'utilisation d'authentification à deux facteurs basée sur des applications mobiles (comme Google Authenticator) ou des clés de sécurité matérielles (U2F, WebAuthn) en raison des préoccupations de sécurité liées aux SMS. Ces méthodes offrent généralement un niveau de sécurité plus élevé et sont moins vulnérables aux attaques.

4.3.6 Authentification d'application mobile

Les applications mobiles dédiées, telles que Google Authenticator ou Authy, peuvent être utilisées pour générer des codes 2FA. Elles sont souvent basées sur les protocoles TOTP ou HOTP. Ces applications offrent une solution pratique et sécurisée pour renforcer le processus d'authentification en ajoutant un deuxième facteur, généralement un code à usage unique, en plus du mot de passe standard.

Voici quelques points clés sur l'utilisation de ces applications dans le contexte de l'authentification à deux facteurs :

- **Génération de codes à usage unique**, ces applications génèrent des codes à usage unique basés sur le protocole TOTP (Time-Based One-Time Password) ou HOTP (HMAC-Based One-Time Password). Ces codes changent régulièrement, ajoutant une couche de sécurité dynamique ;

- **Synchronisation avec le serveur,** lors de la configuration de 2FA sur un service en ligne, l'utilisateur enregistre généralement son appareil mobile en scannant un code QR ou en entrant manuellement une clé secrète. Cette clé secrète est utilisée pour synchroniser l'horloge entre l'application et le serveur d'authentification ;
- **Protection de la clé secrète,** la clé secrète partagée entre l'application et le serveur d'authentification doit être protégée de manière sécurisée. Si cette clé est compromise, l'efficacité du deuxième facteur est compromise. Les utilisateurs sont souvent encouragés à protéger leurs appareils mobiles avec des méthodes de sécurité, comme le verrouillage par code ou la biométrie ;
- **Utilisation avec divers services,** les applications d'authentification à deux facteurs ne sont généralement pas liées à un seul service. Les utilisateurs peuvent utiliser la même application pour plusieurs comptes en configurant chaque service avec sa propre entrée de clé secrète ;
- **Commodité et accessibilité,** ces applications offrent une alternative pratique aux méthodes de 2FA basées sur SMS, et elles ne dépendent pas d'une connexion Internet ou de la réception de messages texte. Cela les rend particulièrement utiles dans des contextes où la connectivité peut être limitée ;
- **Multi-dispositif,** certains services permettent aux utilisateurs de synchroniser leurs configurations 2FA sur plusieurs appareils. Cela peut être utile pour les utilisateurs qui utilisent plusieurs appareils mobiles ou qui veulent assurer la continuité en cas de perte ou de remplacement de leur appareil principal.

Ces applications mobiles dédiées sont un moyen efficace et populaire d'intégrer l'authentification à deux facteurs, offrant un équilibre entre sécurité renforcée et facilité d'utilisation pour les utilisateurs.

4.3.7 Sécurité des communications

L'utilisation de protocoles sécurisés tels que HTTPS (Hypertext Transfer Protocol Secure) est cruciale pour garantir la sécurité des communications entre l'utilisateur et le serveur d'authentification. HTTPS est la version sécurisée du protocole HTTP, et il ajoute une couche de chiffrement SSL/TLS (Secure Sockets Layer/Transport Layer Security) pour protéger les données transitant entre le client (utilisateur) et le serveur. Voici quelques raisons pour lesquelles HTTPS est essentiel pour prévenir les attaques d'interception et renforcer la sécurité des communications :

- **Chiffrement des données,** HTTPS chiffre les données transitant entre le client et le serveur, garantissant ainsi que même si un attaquant intercepte les données, il ne peut pas les lire sans la clé de déchiffrement appropriée. Cela protège la confidentialité des informations sensibles, y compris les identifiants d'authentification ;
- **Protection contre l'interception,** en l'absence de chiffrement, les données transmises sur un réseau non sécurisé, tel qu'Internet, peuvent être interceptées facilement. HTTPS protège contre ces interceptions malveillantes, notamment les attaques de type "Man-in-the-Middle" (MitM) ;
- **Authentification du serveur,** HTTPS utilise des certificats numériques pour authentifier le serveur auprès du client. Cela garantit que le client communique réellement avec le serveur prévu et non avec un imposteur ;
- **Confiance de l'utilisateur,** la présence du cadenas dans la barre d'adresse du navigateur et le préfixe "https://" indiquent aux utilisateurs que la

connexion est sécurisée. Cela renforce la confiance des utilisateurs envers le site ou l'application ;

- **Conformité aux normes de sécurité**, de nombreuses normes de sécurité et réglementations exigent l'utilisation de HTTPS pour le traitement de données sensibles. Cela inclut des normes telles que le RGPD (Règlement Général sur la Protection des Données) et les meilleures pratiques de sécurité telles que celles émises par l'OWASP (Open Web Application Security Project) ;
- **Protection contre les attaques actives**, HTTPS protège contre les attaques actives où un attaquant tente de modifier les données en transit. Le chiffrement garantit l'intégrité des données et détecte toute altération non autorisée ;
- **Utilisation de certificats SSL/TLS forts**, le choix de certificats SSL/TLS forts et la mise en œuvre correcte des protocoles de chiffrement contribuent à renforcer la sécurité de la connexion.

L'utilisation de HTTPS est une mesure fondamentale pour garantir la sécurité des communications, en particulier lorsqu'il s'agit d'authentification où des informations sensibles sont échangées entre l'utilisateur et le serveur. C'est un élément essentiel pour créer un environnement en ligne sûr et sécurisé.

4.3.8 Politiques de réinitialisation et de récupération

Absolument, les politiques de réinitialisation et de récupération jouent un rôle essentiel dans la gestion des comptes d'utilisateurs, en particulier lorsqu'il s'agit de l'authentification à deux facteurs (2FA). Ces politiques visent à garantir que les utilisateurs peuvent récupérer l'accès à leur compte de manière sécurisée, tout en

minimisant les risques de compromission. Quelques éléments à considérer pour des politiques robustes de réinitialisation et de récupération :

- **Validation de l'identité**, lorsqu'un utilisateur souhaite réinitialiser ou récupérer son compte, des mécanismes de validation d'identité robustes doivent être en place. Cela peut inclure l'envoi d'un code de réinitialisation à une adresse e-mail préalablement enregistrée, la réponse à des questions de sécurité prédéfinies, ou d'autres méthodes de confirmation d'identité ;
- **Utilisation de méthodes multiples**, proposer plusieurs méthodes de réinitialisation et de récupération pour s'adapter aux préférences et aux situations des utilisateurs. Cela peut inclure des options telles que la réinitialisation par e-mail, par SMS, par appel téléphonique, ou par l'intermédiaire d'une application mobile ;
- **Politiques de sécurité pour la réinitialisation**, établir des politiques de sécurité claires pour la réinitialisation des comptes. Cela peut inclure des délais de temporisation, des limitations sur le nombre de tentatives, et la nécessité de valider l'identité avant de procéder à une réinitialisation ;
- **Utilisation de codes de sécurité**, lors de la réinitialisation, l'utilisation de codes de sécurité uniques et temporaires peut renforcer la sécurité du processus. Ces codes peuvent être envoyés via des canaux sécurisés tels que SMS ou e-mail ;
- **Communication sécurisée**, veiller à ce que toutes les communications liées à la réinitialisation et à la récupération soient effectuées de manière sécurisée, de préférence via des canaux chiffrés. Les liens de réinitialisation ne devraient pas être transmis de manière non sécurisée ;
- **Formation des utilisateurs**, fournir aux utilisateurs des informations et une formation sur la manière sécurisée de réinitialiser leur compte. Cela peut

contribuer à réduire les risques d'ingénierie sociale ou d'attaques de récupération de compte ;

- **Gestion des comptes inactifs**, définir des politiques de gestion des comptes inactifs, y compris la manière dont les comptes sont désactivés ou supprimés après une période d'inactivité prolongée ;
- **Historique des réinitialisations**, tenir un historique des réinitialisations et des récupérations de compte, accessible aux administrateurs. Cela peut être utile pour détecter des activités suspectes ou des tentatives d'usurpation de compte ;
- **Mécanismes de secours**, envisager des mécanismes de secours pour les utilisateurs qui pourraient perdre l'accès à leur dispositif 2FA principal. Cela peut inclure la fourniture de codes de secours ou d'autres méthodes alternatives ;
- **Conformité aux normes de sécurité**, assurer la conformité aux normes de sécurité et aux réglementations pertinentes liées à la gestion des comptes utilisateur, telles que le RGPD.

En mettant en œuvre des politiques de réinitialisation et de récupération robustes, les organisations peuvent fournir aux utilisateurs des mécanismes flexibles tout en maintenant un niveau élevé de sécurité pour protéger les comptes contre un accès non autorisé.

En combinant ces protocoles et technologies, le système d'authentification 2FA peut offrir une protection supplémentaire contre les accès non autorisés en exigeant la vérification de l'identité de l'utilisateur à l'aide de deux facteurs distincts.

4.4 Conclusion

En somme dans ce chapitre, nous avons présenté le système d'authentification à double facteurs en long et en large, tout en passant par un aperçu approfondie sur son fonctionnement et de son architecture interne. Le chapitre prochain présentera les détails sur l'implémentation du système d'authentification à double facteurs.

CHAPITRE 5 : MISE EN ŒUVRE DU SYSTEME D'AUTHENTIFICATION

5.1 Introduction

Ce chapitre concerne les différentes étapes de déploiement de la solution. Il partira de comment installer le logiciel UserLock, ensuite les configurations nécessaires sur ce logiciel pour mettre en place un système, puis nous allons passer à la mise en place de notre système d'authentification à double. Dans ce chapitre nous donnerons une estimation du coût de sa réalisation.

5.2 Installation et Configuration

5.2.1. Prérequis [15]

Configuration requise

- **Domaine**

Active Directory requis (sauf en cas de Serveur UserLock de Terminal indépendant).

Niveau fonctionnel de la forêt et du domaine : Windows Server 2003 ou plus récent.

- **Système d'exploitation**

Tableau 3: Les systèmes compatibles avec UserLock 12.0 [9]

	Serveur UserLock	Console UserLock	Fonctionnalité MFA	Servic e SSO	Pour postes de travail à protéger	Pour serveurs de terminaux à protéger	Pour les serveurs NPS et IIS
Versions Client Windows							
Windows 11		✓	✓		✓		
Windows 10 Build 1803		✓	✓		✓		

	Serveur UserLock	Console UserLock	Fonctionnalité MFA	Service SSO	Pour postes de travail à protéger	Pour serveurs terminaux à protéger	Pour les serveurs NPS et IIS
Windows 10		✓	✓		✓		
Windows 8.1		✓	✓		✓		
Windows 8		✓	✓		✓		
Windows 7		✓	!		✓		
Versions Windows Serveur							
Windows Serveur 2022	✓	✓	✓	✓		✓	✓
Windows Serveur 2019	✓	✓	✓	✓		✓	✓
Windows Serveur 2016	✓	✓	✓	✓		✓	✓
Windows Serveur 2012 R2	✓	✓	✓	✓		✓	✓
Windows Serveur 2012	✓	!	!			✓	✓
Windows Serveur 2008 R2						✓	✓

- **Services et protocoles réseaux Windows**

- Le service 'Registre à distance'.
- Le service UserLock.

- Le protocole ICMP (ping).
- Le protocole 'Partage de fichiers et d'imprimantes' Microsoft (SMB TCP 445).
- **Matériel.**
 - CPU & RAM
 - Espace disque
 - Connexion réseau
- **Base de données.**

L'ensemble de l'activité des sessions utilisateur est audité par UserLock et sauvegardé dans une base de données à des fins d'analyse et de reporting.

UserLock supporte les systèmes de base de données suivants :

- MS Access mdb file.
- MS SQL Express 2005 et supérieurs - 32/64 bits.
- Microsoft SQL Server 2008 supérieurs.
- MySQL 5.6 et supérieurs.

✎ *Les versions/éditions MS SQL LocalDB ne sont pas supportées.*

5.2.2. Installation et configuration dans Windows server 2019

- Adressage :
 - Adresse réseau @192.168.100.0
 - Adresse server @192.168.100.10
 - Adresse machine client @192.168.100.102
 - Adresse DNS @192.168.100.10
- Installation des services :
 - AD DS
 - DHCP
 - DNS
- Configuration :
 - Nom du domaine : centre-muraz.local
 - Nom du server : SERVER
 - Machine client : Windows 10
 - Nom machine client : ZOURE

- Groupes et utilisateurs :
 - Groupe : SSQIE (utilisateurs : Secrétaire et Informaticien)
 - Utilisateur : Abdramane
- Base de données : Création d'une base de données MySQL avec Wampserver3.3.2 64bits.

5.2.3. Architecture de déploiement

Dans le cadre de notre étude, le déploiement de la solution se fera sur le logiciel userlock installer sur un système d'exploitation Windows Server 2019. La **figure 5** présente l'architecture de déploiement dans l'environnement de test du Centre MURAZ.

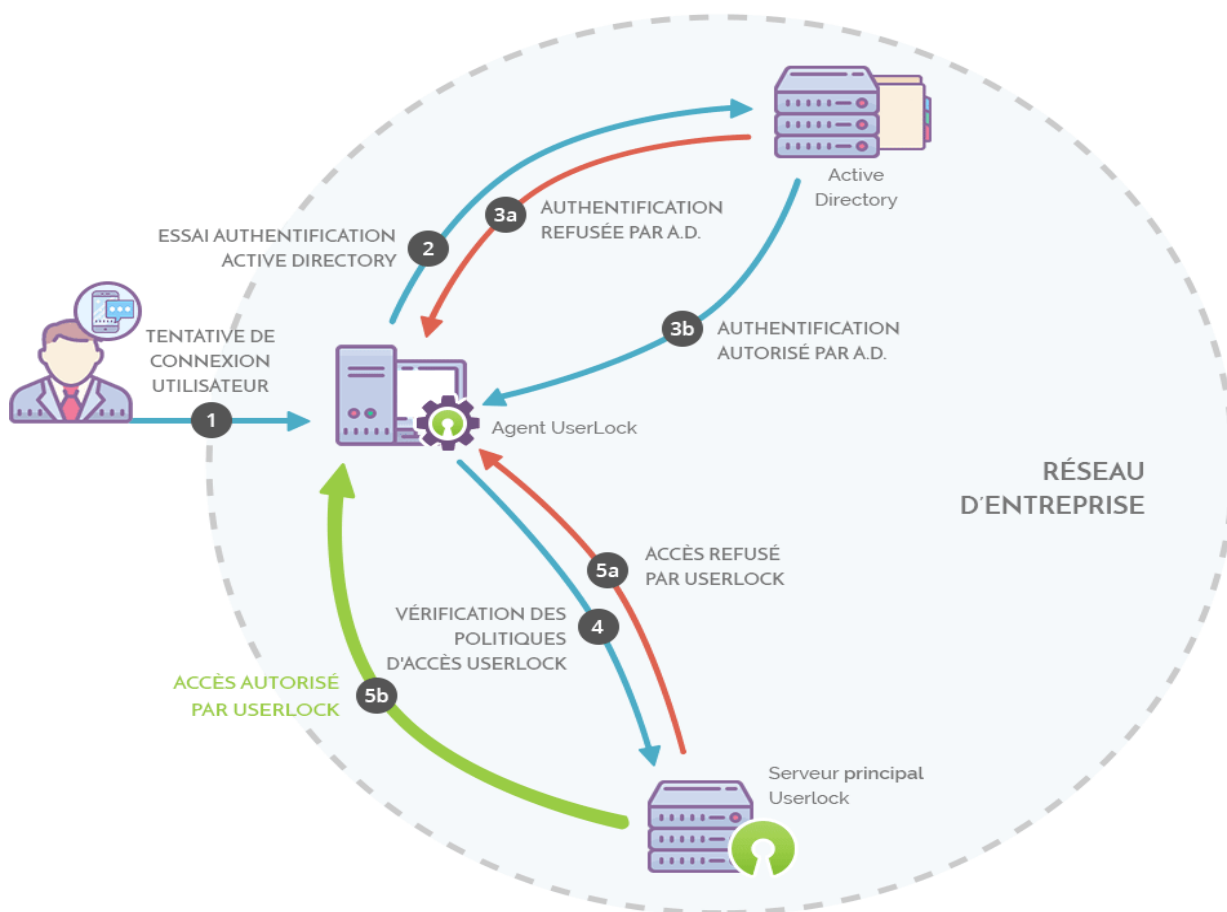


Figure 5: Architecture de déploiement [8]

L'architecture est constituée de :

- ❖ 1 serveur principal ;
- ❖ 1 machine virtuelle ;
- ❖ 1 smartphone ;
- ❖ 1 contrôleur de domaine native au serveur Windows.

5.2.4. Estimation du coût de déploiement

Afin de définir et appliquer les besoins d'accès légitimes pour tous les utilisateurs, le nombre de sessions utilisateurs estimé est environ 100 sessions au sein du Centre MURAZ. Ainsi le choix de la licence **UserLock 12.0** serait alors nécessaire. Vu que UserLock peut traiter jusqu'à 100 événements de connexion par seconde avec un processeur double cœur. Avec une fréquence de connexion de 2 GHz il est possible d'authentifier 6000 utilisateurs par minute. Le **tableau 4** présente les ressources dont nous aurons besoin pour la mise en place de notre solution.

Tableau 4: Estimation des coûts de réalisation [10] [11]

Désignations	Coûts en Franc CFA
Server Windows 2019	1 264 900
Licence UserLock	1 015 360/ans
Main d'œuvre	500 000
Formation de l'administrateur	900 000
Total	3 680 260

Ces coûts de réalisations sont des estimations au cours des prestations d'installation chez les particuliers car ici en entreprise sauf licence toutes les autres ressources sont déjà disponibles. La formation de l'administrateur se fera sur trois (03) jours à raison de 300 000 FCFA/ jour.

5.2.5. Installation et configuration de UserLock

5.2.5.1 Installation de UserLock

UserLock est une application Windows dont l'installation est faite juste en cliquant sur l'application. Il peut être installé sur un serveur. Lors de l'installation il faut :

- ✓ Choisir le langage d'installation ;
- ✓ Valider le contrat de licence ;
- ✓ Entrez votre adresse email ;
- ✓ Insérer le nom et la clé de licence ;
- ✓ Choisir le dossier d'installation ;
- ✓ Attendre la fin de l'installation ;

Une fois l'installation terminée, un 'Assistant de configuration' s'ouvre pour nous guider dans la configuration de UserLock.

5.2.5.2 Configuration de UserLock

On sélectionne 'CONTINUER' pour commencer la configuration du service et des modules de UserLock.

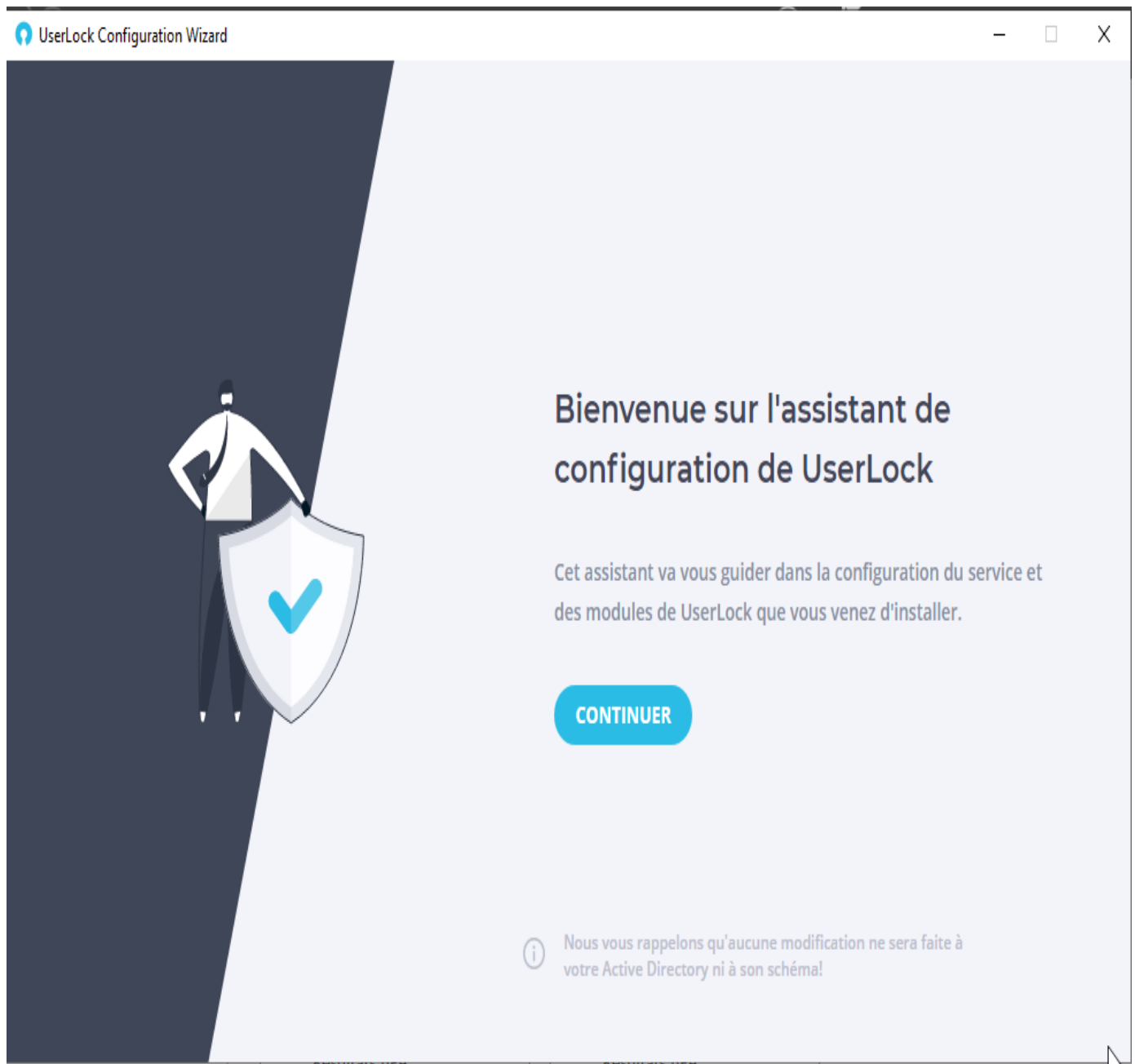


Figure 6: Page d'accueil de configuration UserLock

On clique sur 'DEMARRER' pour la configuration du serveur qui est obligatoire.

Ceci étant notre première installation de l'application, on conserve 'Serveur principal' sélectionné et on clique sur 'Suivant'.

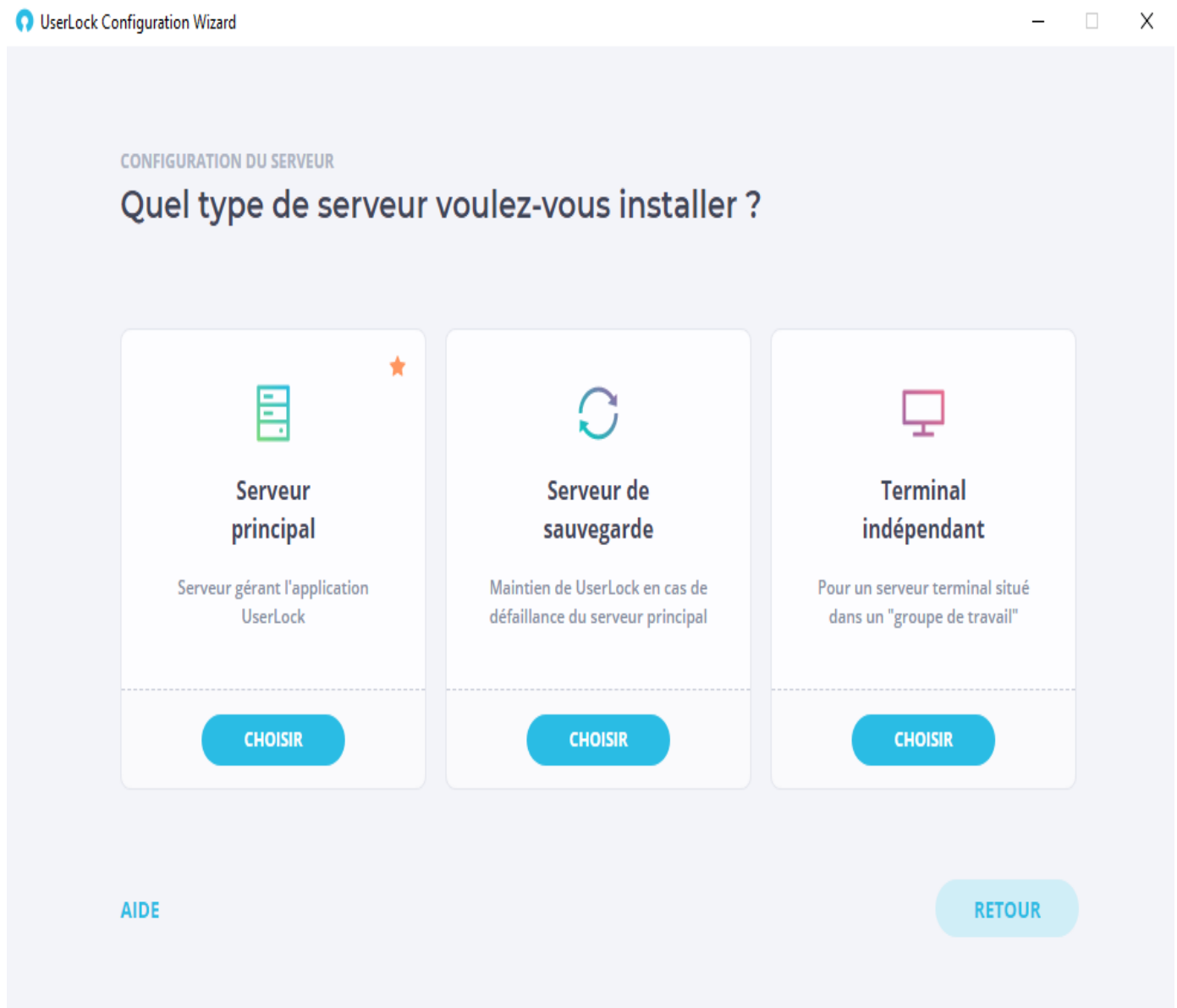


Figure 7: Type de serveur

On sélectionne la zone réseau dont les accès seront surveillés par UserLock. Nous pouvons choisir d'auditer et de contrôler les accès sur tout le réseau ou on sélectionne des unités organisationnelles machines spécifiques. On clique sur 'Suivant'.

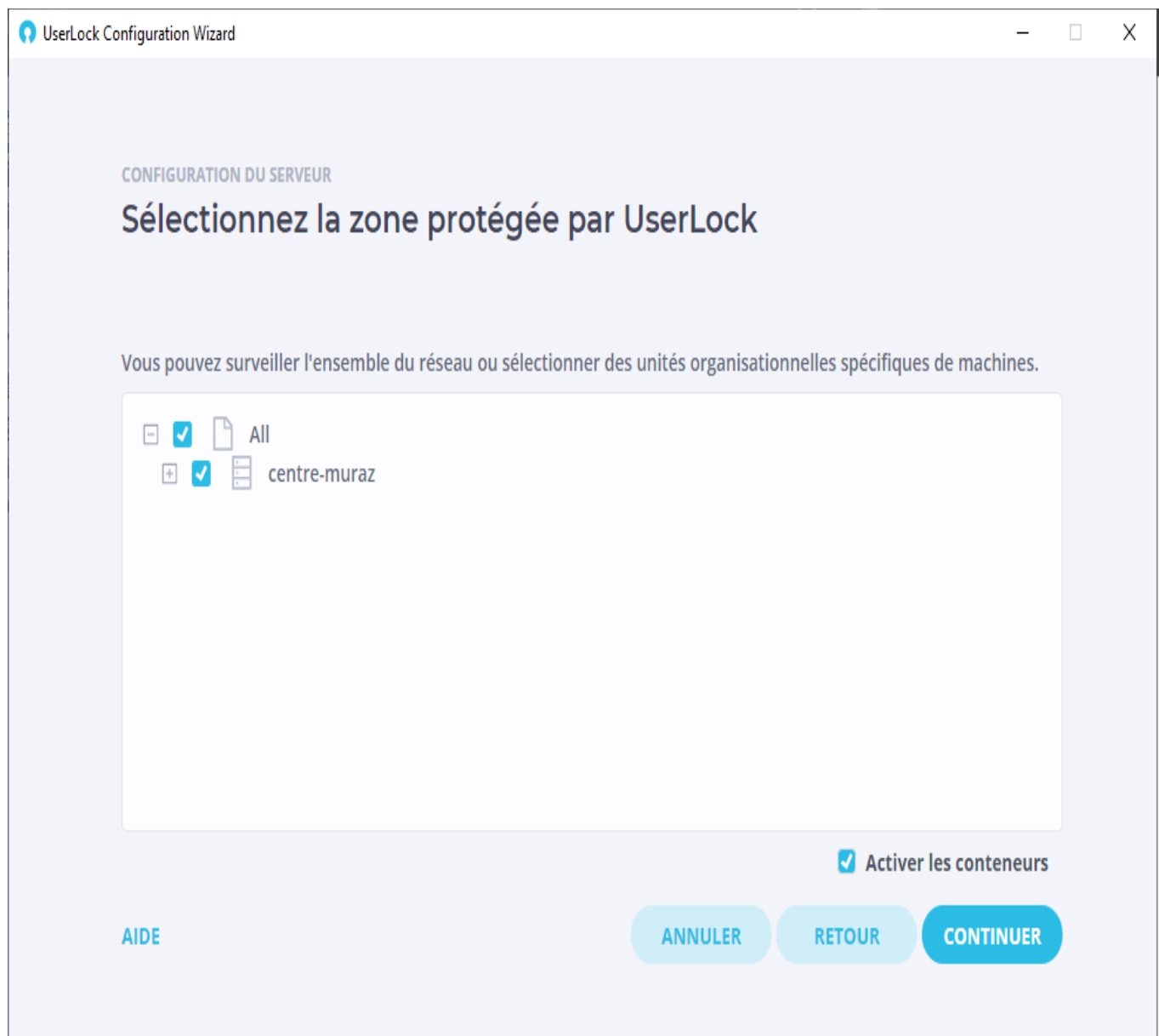


Figure 8: Zone à protéger par Userlock

UserLock a besoin de se dépersonnaliser à l'aide d'un compte ayant les droits d'administration sur les machines protégées afin de procéder à l'installation des agents ou interagir avec les sessions et les machines à distance. Aucune modification ne sera faite à votre Active Directory ou à son schéma. On spécifie le compte administrateur à utiliser dans ces cas spécifiques et on clique sur 'Suivant'.

The screenshot shows a web-based configuration wizard titled 'UserLock Configuration Wizard'. The main heading is 'CONFIGURATION DU SERVEUR' followed by 'Compte de dépersonnalisation du service'. On the left, there is explanatory text in French: 'Le service UserLock s'exécutera avec le compte SERVICE RÉSEAU avec le minimum de privilèges, mais a besoin d'un **compte de dépersonnalisation** ayant les **droits d'administration** sur les machines à protéger.' Below this, it says 'Sélectionnez le compte que UserLock utilisera pour accéder aux machines à protéger.' On the right, there are three input fields: 'Domaine' with the value 'CENTRE-MURAZ', 'Compte' with the value 'Administrateur', and 'Mot de passe' which is masked with dots and has a visibility icon. At the bottom, there is an 'AIDE' link and three buttons: 'ANNULER', 'RETOUR', and 'CONTINUER'.

Figure 9: Identification du compte de dépersonnalisation

La configuration du serveur UserLock est finie. On clique sur 'Continuer'.

Sur l'interface suivante, on clique sur 1^{er} bouton pour continuer à configurer les modules installés ou ouvrir la console d'administration sur le 2^{ème} bouton.

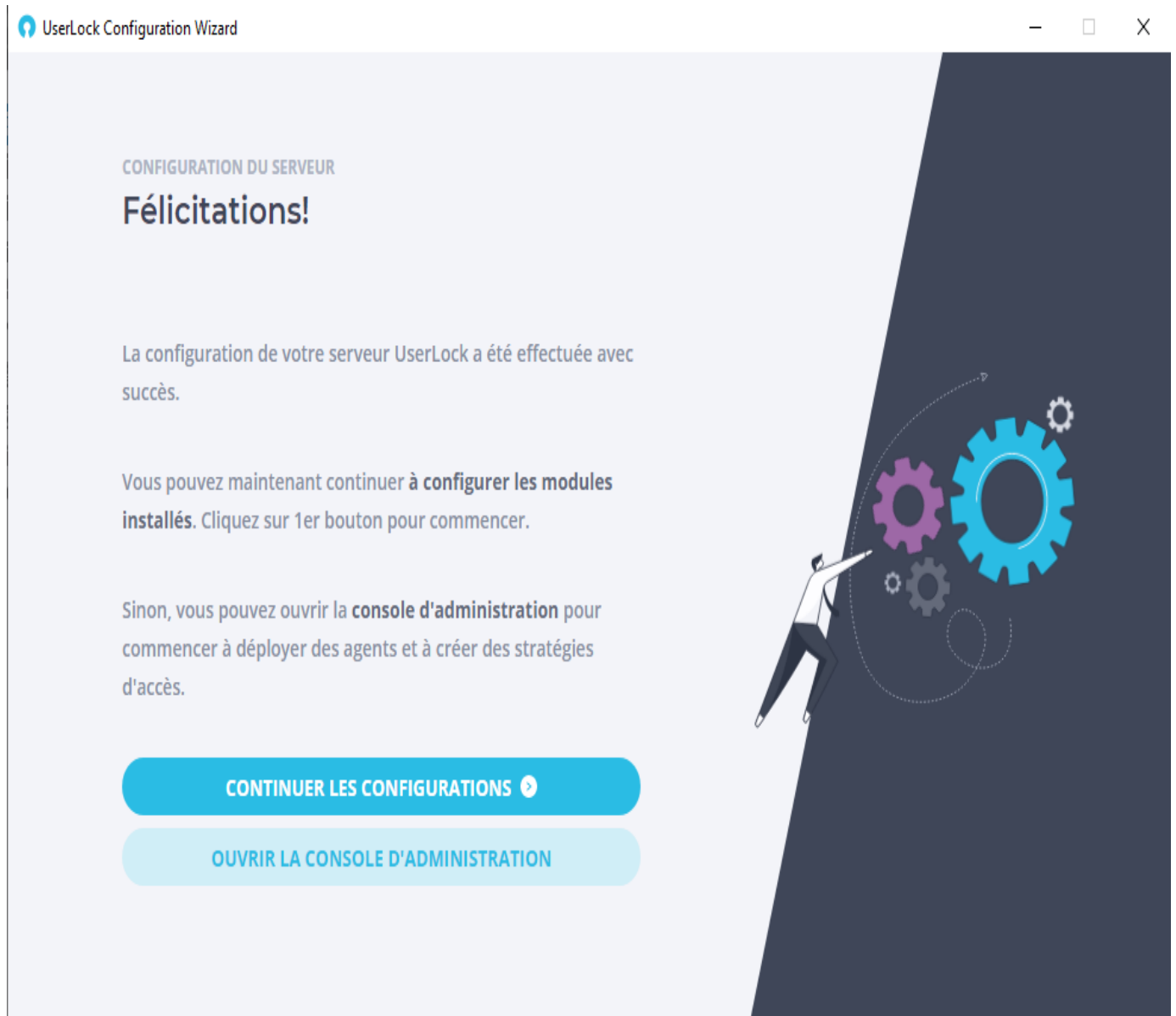


Figure 10: Fin de configuration

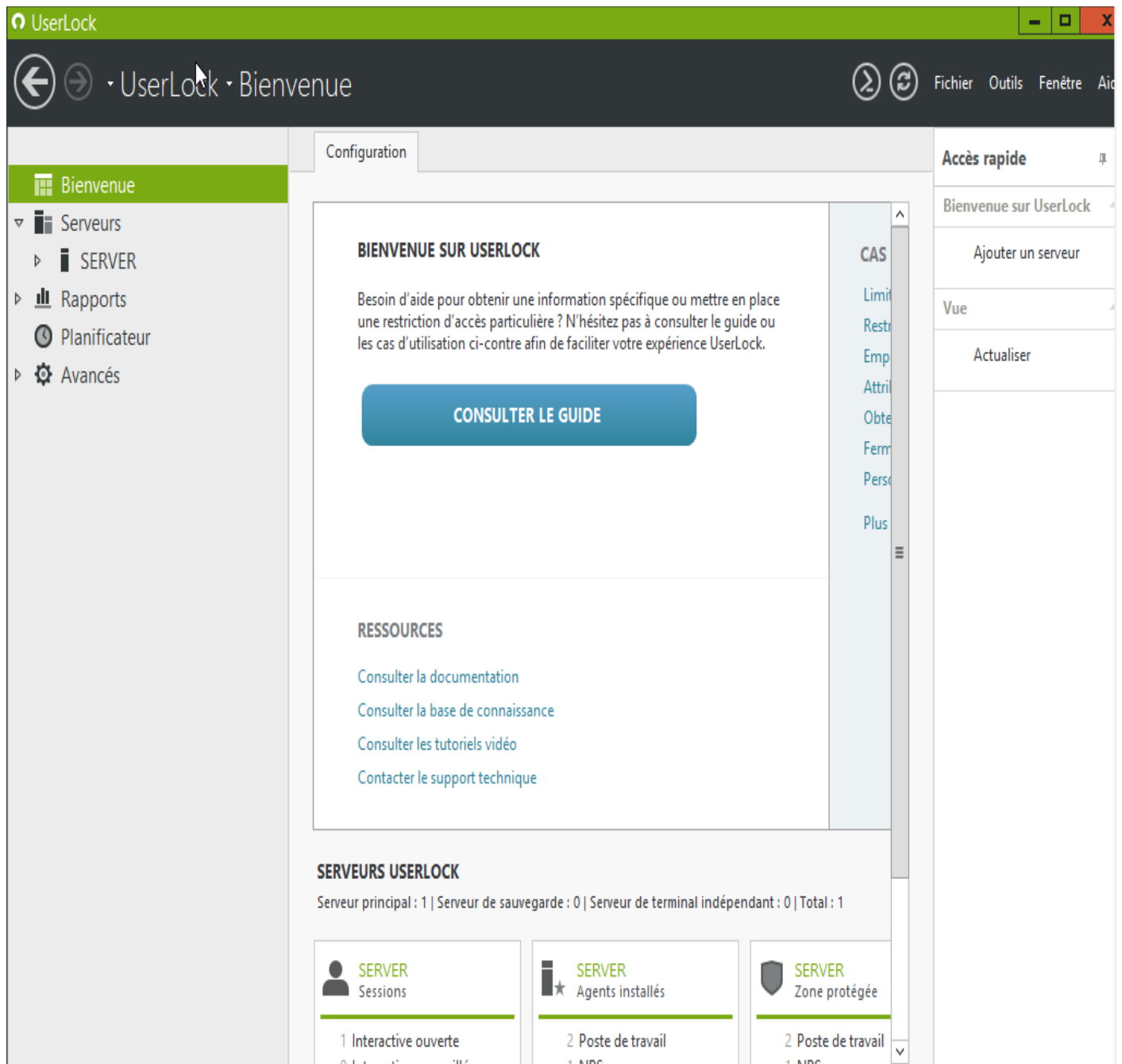


Figure 11: Page d'accueil UserLock

5.2.6. Mise en place de la base de données de production

Pour définir notre base de données de production :

- Création d'une base de données vide au sein de notre système de base de données MySQL.

- Dans la console UserLock, on sélectionne notre serveur UserLock dans le menu de gauche puis on clique sur 'Propriétés' dans le panneau 'Accès rapide'.
- On Affiche la section 'Base de données'.
- Vérifions que la case 'Enregistrer tous les événements dans une base de données' est bien cochée. Cette option doit être activée pour tous les événements de connexions soient sauvegardés dans la base de données UserLock.

On sélectionne 'Autre base de données' et on clique sur le bouton à droite du champ de saisie pour lancer l'assistant qui nous guidera.

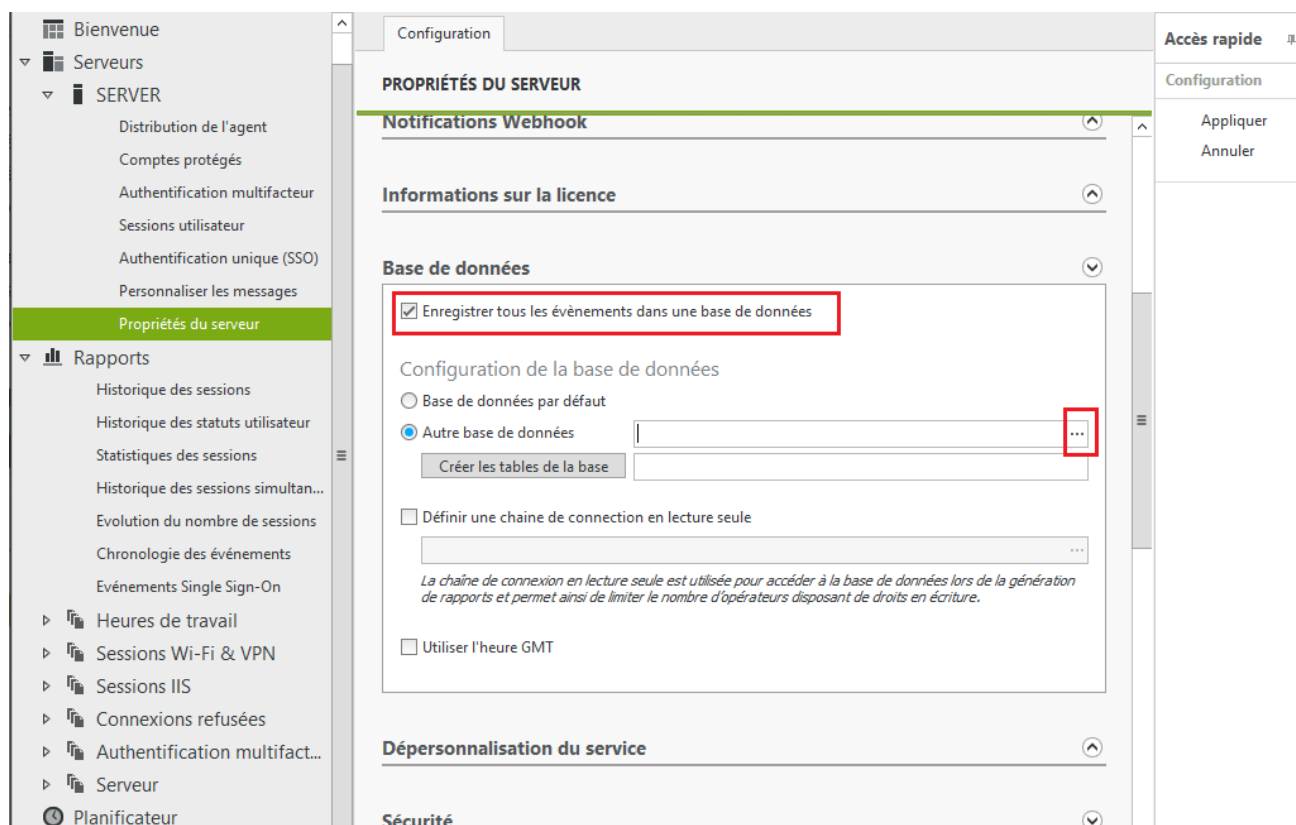


Figure 12: Choix de la base de données

On sélectionne notre système de base de données et on clique sur 'OK'.

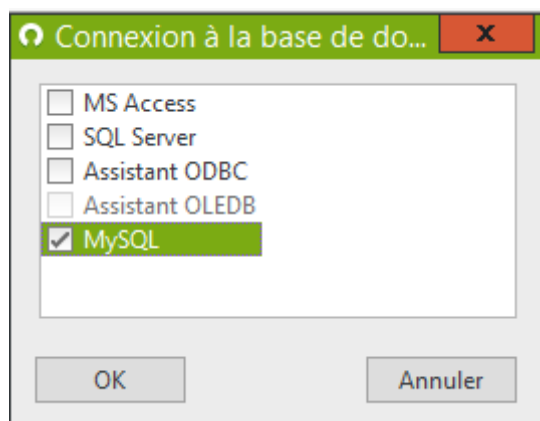


Figure 13: Connexion à la base de données

On saisit les informations de connexion et on précise un compte utilisateur possédant les droits de création de tables sur la base de données. Puis on sélectionne la base de données que nous avons précédemment créée durant l'étape 1.

On clique sur le bouton 'Test' pour vérifier la connexion, et valider les informations saisies en cliquant sur 'OK' si le test est concluant.

On clique sur 'Créer les tables de la base'. Cette opération de création des tables ne doit être effectuée que lorsqu'une nouvelle base de données vide est configurée.

La nouvelle base de données est définie. On clique sur 'Appliquer' dans le panneau 'Accès rapide' pour valider les paramètres.

5.2.7. Déploiement d'agents

5.2.7.1 Déploiement manuel des agents

On sélectionne 'Agent distribution' dans le menu de gauche.

Cette vue affiche toutes les machines détectées dans la zone réseau surveillée par UserLock.

On sélectionne les machines cibles en cliquant sur leur ligne correspondante tout en maintenant la touche 'Ctrl' appuyée. Puis on clique sur 'Installer' depuis le panneau 'Accès rapide' affiché sur notre droite.

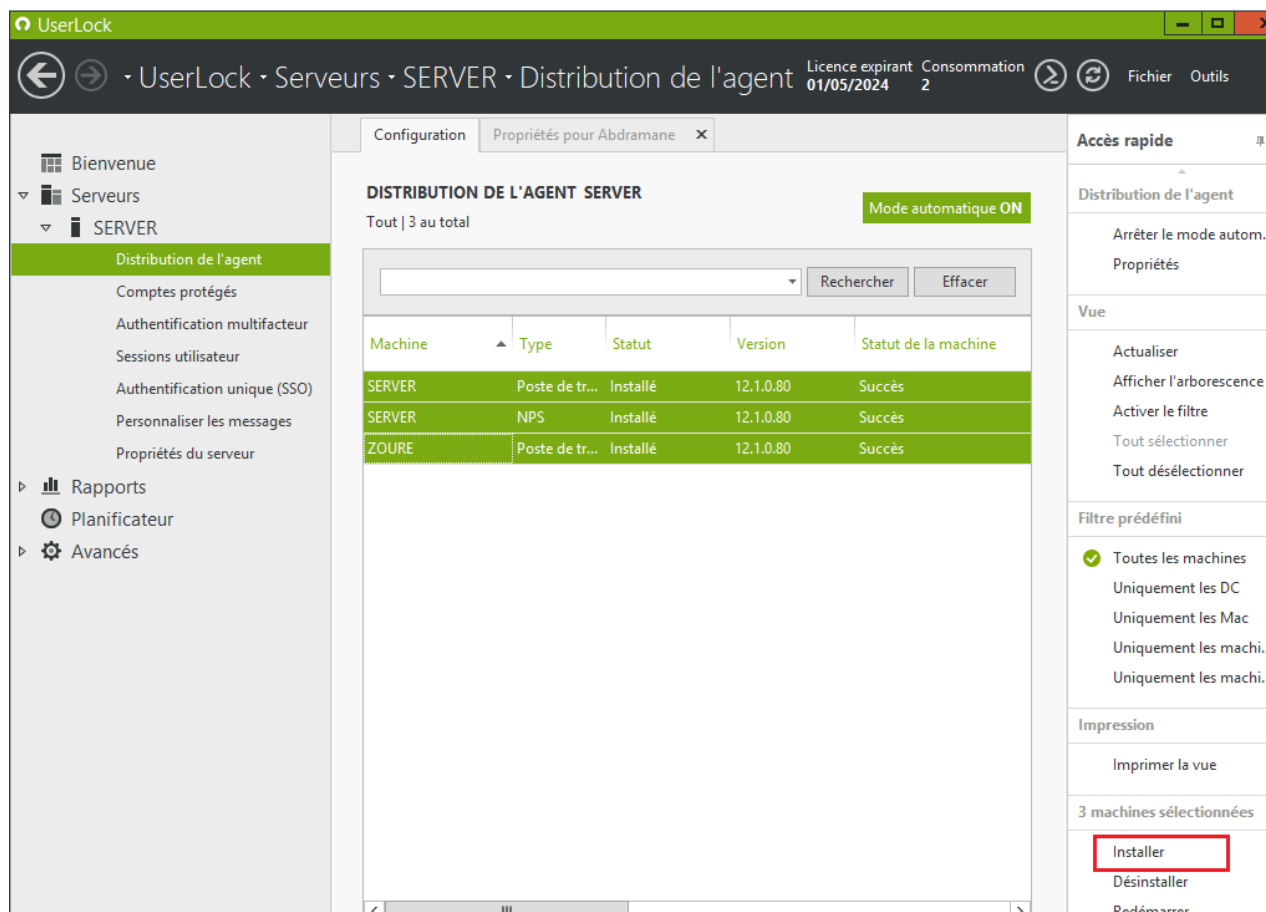


Figure 14: Installation des agents

Différentes options d'affichage sont disponibles pour nous permettre de personnaliser la vue si la liste affichée ici est trop longue. Nous pouvons changer l'affichage des données depuis le panneau 'Accès rapide' en sélectionnant l'un des filtres prédéfinis ou directement depuis les options proposées dans l'entête de chaque colonne de la grille de données.

Une fois l'installation lancée, un nouvel onglet s'ouvre dans la fenêtre centrale pour afficher la progression de l'installation et le résultat.

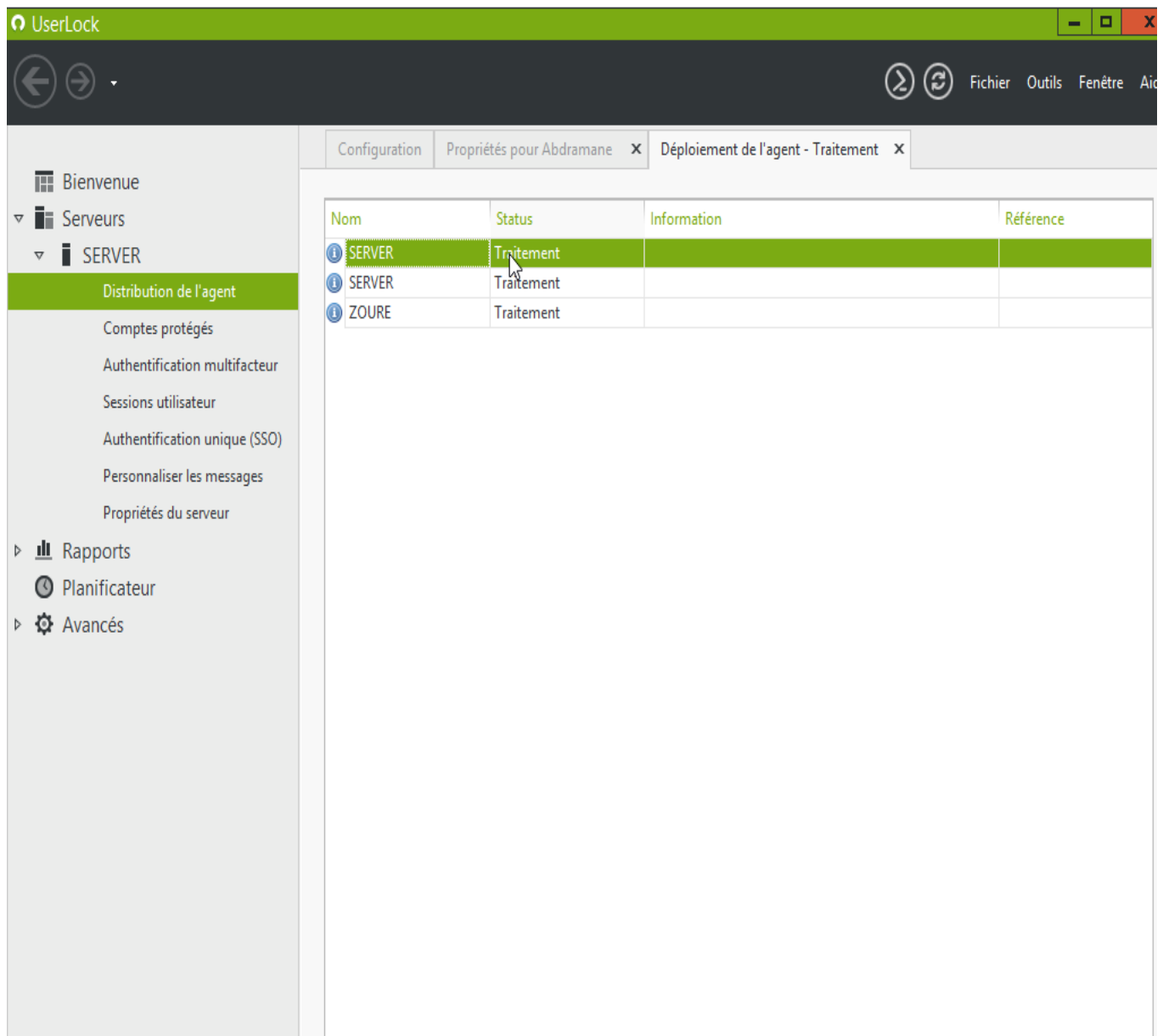


Figure 15: Progression de l'installation des agents

Si une erreur se produit, comme par exemple un prérequis manquant, un message sera alors affiché pour la machine concernée ainsi que des indications pour résoudre le problème.

On ferme cet onglet pour revenir sur la vue précédente et on clique sur 'Actualiser' depuis le panneau 'Accès rapide'.

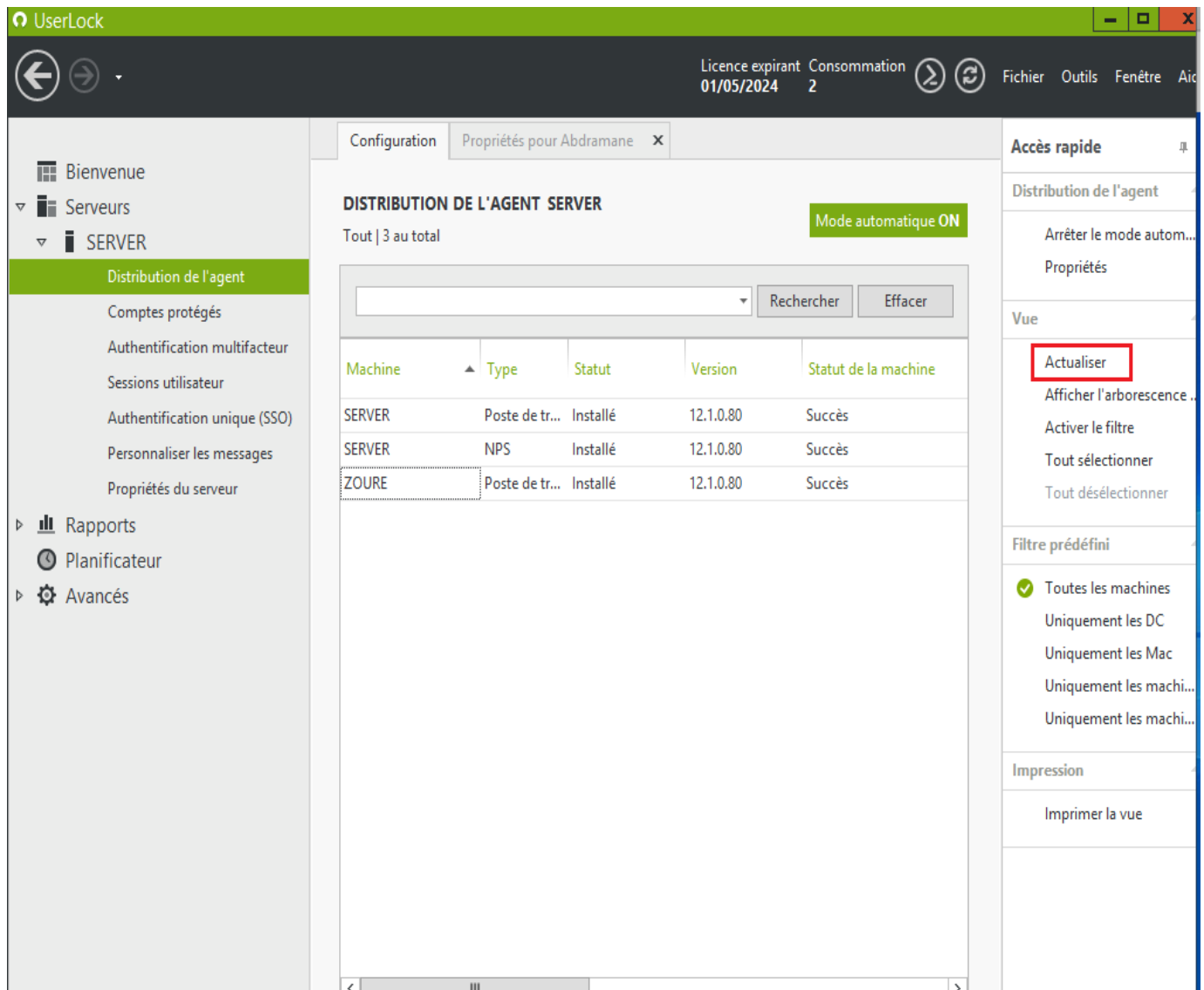


Figure 16: Liste des Agents installés

L'agent 'Station' est maintenant installé sur les machines sélectionnées. Dès lors, toutes les connexions d'accès sur ces machines sont auditées et sauvegardées dans la base de données UserLock.

UserLock propose différents types d'agents en fonction du type de session à contrôler. Une même machine, comme un serveur par exemple, peut recevoir plusieurs types d'agent (Station, NPS, IIS).

5.2.7.2 Déploiement automatique des agents

Un mode de déploiement automatique est disponible pour installer les agents 'Station' et 'Mac' sur toutes les machines détectées dans la zone réseau surveillée par UserLock. Par défaut, notez que les serveurs sont exclus de ce processus de déploiement automatique.

Sélectionnez 'Agent distribution' dans le menu de gauche.

Cette vue affiche toutes les machines détectées dans la zone réseau surveillée par UserLock. On clique sur le bouton 'Mode automatique' affichée dans l'entête de cette vue.

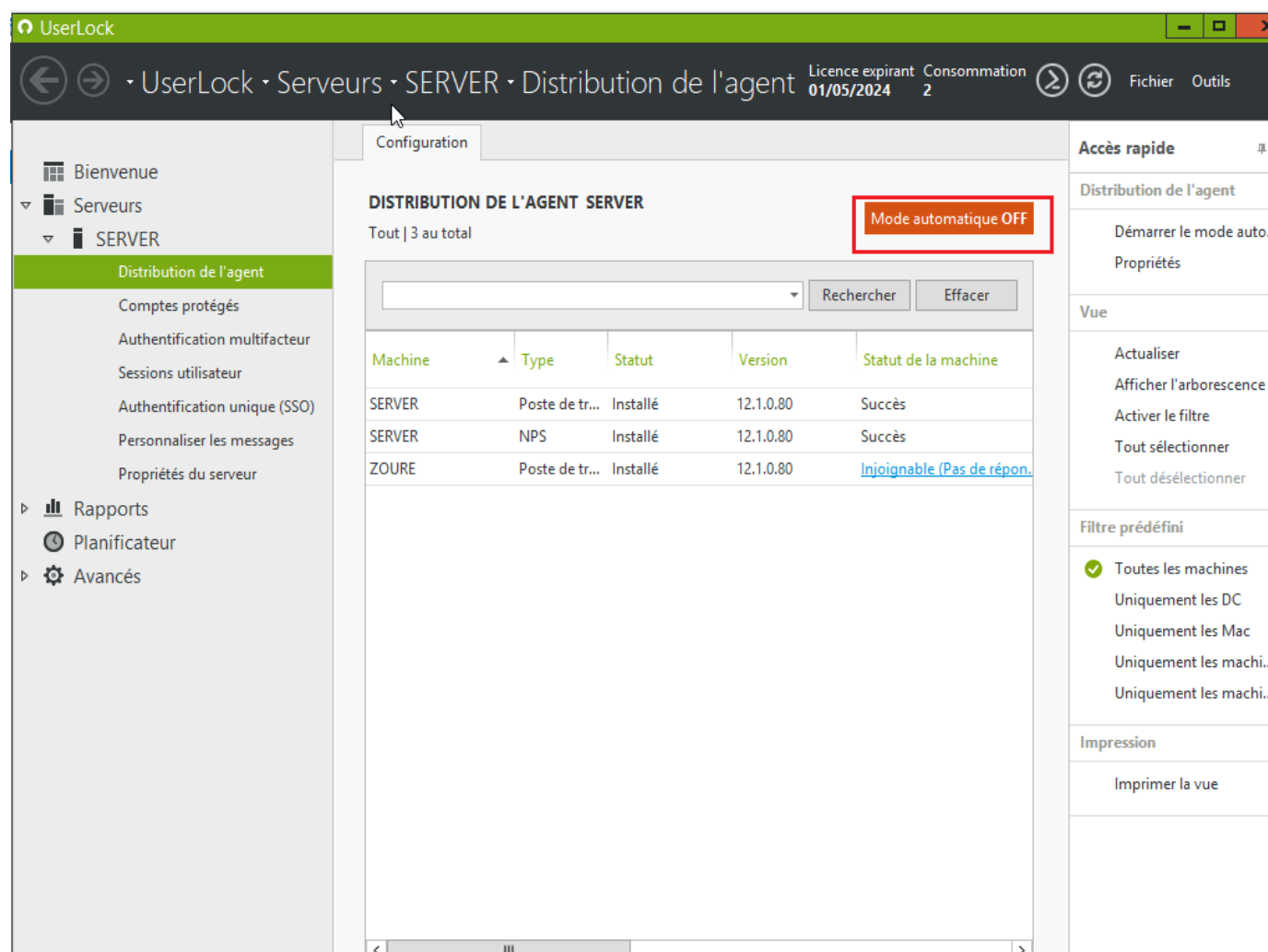


Figure 17: Déploiement automatique des agents

Un message pop-up vous demande alors de confirmer le démarrage du mode automatique. On clique sur 'Oui'.

Par défaut les serveurs sont exclus du périmètre de déploiement automatique.

Le mode automatique est démarré. On clique sur 'OK'.

On clique sur 'Actualiser' dans le panneau 'Accès rapide' après un certain temps pour suivre la progression de l'installation. Ce processus étant exécuté séquentiellement afin de ne pas consommer de ressources et de bande passante, le temps requis pour déployer l'agent 'Station' sur toutes les machines du réseau dépendra du nombre de machines référencées et de leurs disponibilités (joignables ou injoignables).

On note que le bouton 'Mode automatique' a basculé sur 'ON'. On clique à nouveau dessus pour l'arrêter.

5.2.8. Création de compte protégés

Des règles de connexions et des restrictions d'accès peuvent être définies par utilisateur, groupe d'utilisateurs ou unité organisationnelle utilisateur en utilisant une entité UserLock appelé 'Compte protégé'. Cette entité, interne à UserLock, est basée sur les utilisateurs, groupes et unités organisationnelles Active Directory mais ne modifie en aucune manière les comptes Active Directory, ni sa structure ou son schéma.

On clique sur 'Comptes protégés' dans le menu de gauche.

Lorsqu'il existe au moins un compte protégé, cette vue affiche alors les comptes protégés sous la forme d'une liste. Un panneau "Accès rapide" est disponible sur votre droite pour lancer les actions sur les comptes protégés.

Depuis ce panneau, on clique sur le bouton 'Protéger un nouveau compte'.

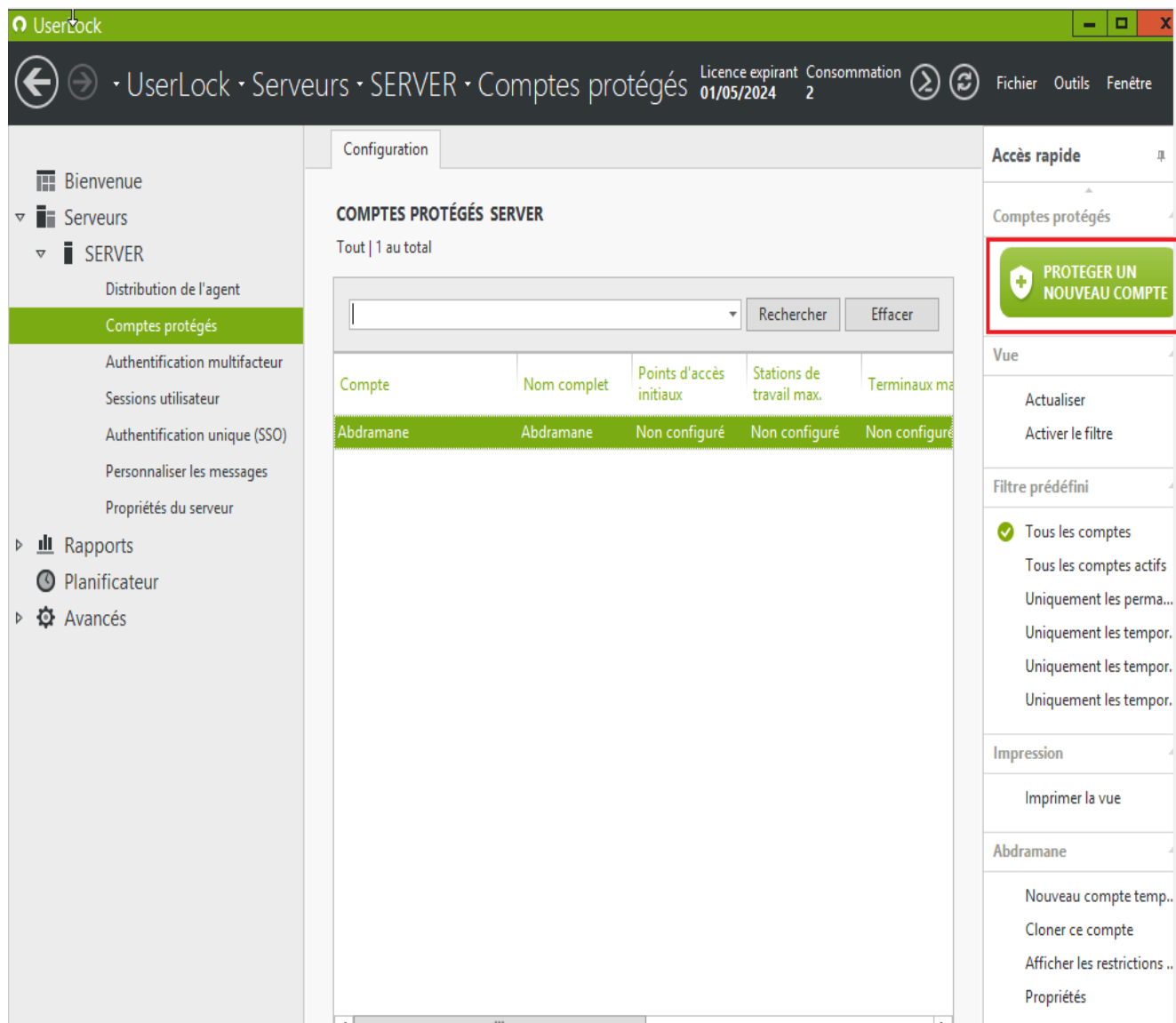


Figure 18: Accueil de comptes protégés

Un assistant s'ouvre alors pour nous guider dans la définition du nouveau compte à protéger. Un bouton 'Mode avancé' est affiché dans le coin inférieur gauche. On clique dessus.

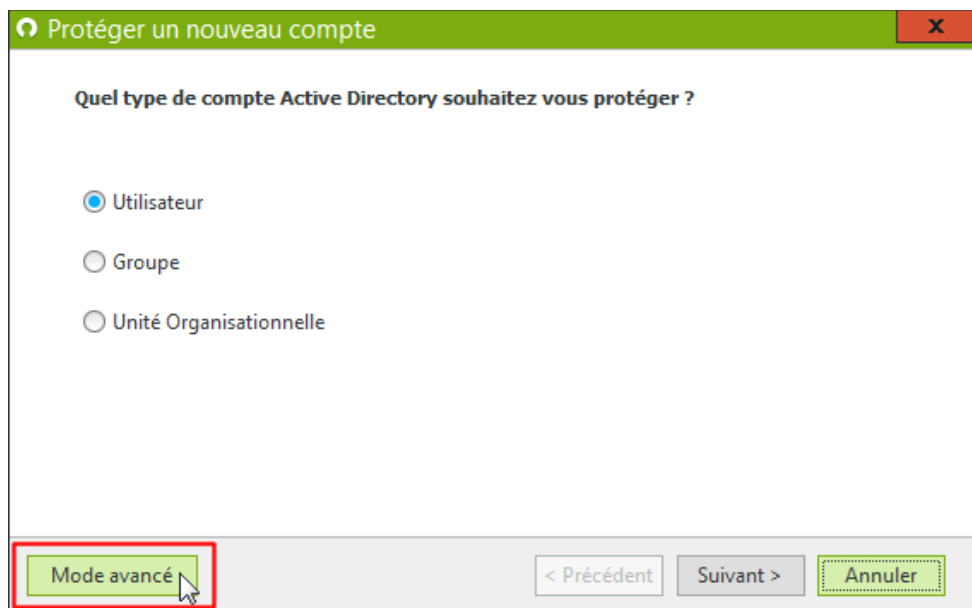


Figure 19: Choix du mode de Création du compte

On sélectionne 'Groupe' dans la liste déroulante comme nouveau type de compte à protéger.

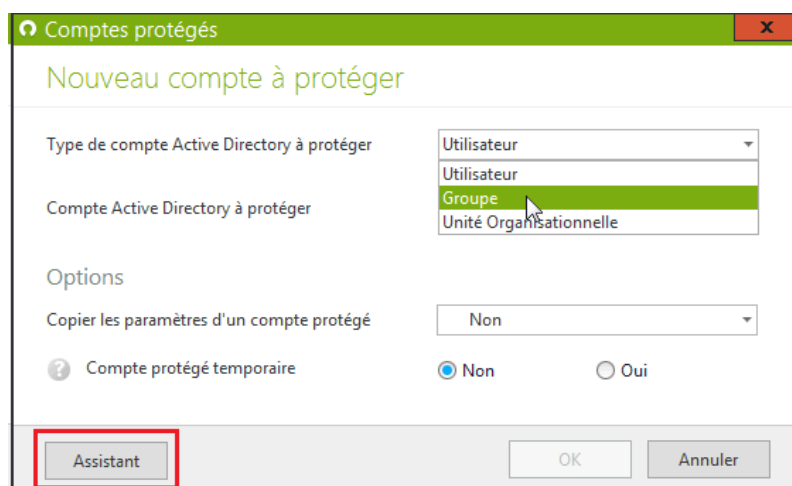


Figure 20: Choix du type de compte à protéger

On note qu'un bouton 'Assistant' est disponible dans le coin inférieur gauche. Cette option permet la création d'un compte protégé en plusieurs étapes.

Dans le champ 'Compte Active Directory à protéger', on saisit le nom exact du groupe que nous souhaitons protéger si nous le connaissons et on clique sur 'Suivant'. Dans le cas contraire, on clique sur le bouton de recherche à droite du champ de saisi pour lancer le sélecteur Active Directory.

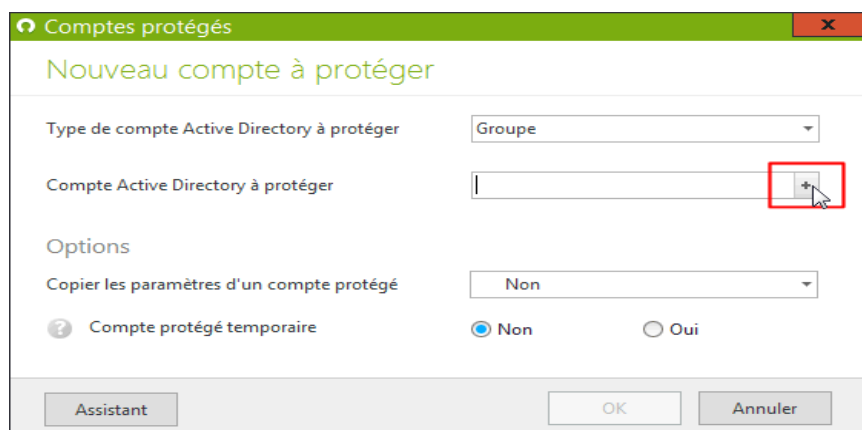


Figure 21: Sélection du compte AD à protéger

On saisit le début du nom du groupe et on clique sur 'Vérifier les noms'. Nous pouvons également lancer le mode 'Avancé...' si nous voulons.

Si le moteur de recherche trouve directement le groupe souhaité, son nom sera alors complété dans le champ de saisi. Dans le cas contraire, une nouvelle fenêtre listera tous les groupes ayant le même début de nom. On sélectionne alors le groupe souhaité dans cette liste et on clique sur 'OK' pour revenir sur l'assistant.

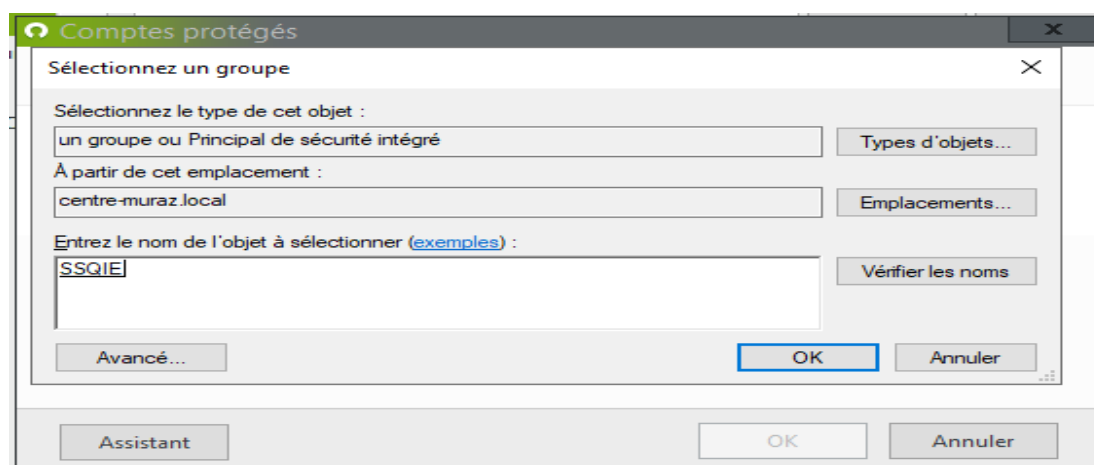


Figure 22: Sélection de l'objet.

On clique sur 'OK' pour valider la définition du compte protégé.

Pour créer un compte protégé temporaire afin de définir des règles valides pour une période de temps donnée, on bascule le bouton radio sur 'Oui' et on ajuste la période de temps souhaitée.

On clique sur 'OK' pour valider la définition du compte protégé qui sera dans ce cas temporaire.

The screenshot shows a Windows-style dialog box titled 'Comptes protégés temporaires' with a green header bar. Below the title bar, the main heading is 'Nouveau compte à protéger'. The dialog contains several configuration fields:

- 'Type de compte Active Directory à protéger': A dropdown menu currently showing 'Groupe'.
- 'Compte Active Directory à protéger': A text box containing 'CENTRE-MURAZ\SSQIE' with a '+' icon on the right.
- 'Options' section:
 - 'Copier les paramètres d'un compte protégé': A dropdown menu showing 'Non'.
 - 'Compte protégé temporaire': Two radio buttons, 'Non' and 'Oui'. The 'Oui' button is selected.
 - 'Heure de début': Two input fields showing '20/02/2024' and '00:00:00'.
 - 'Heure de fin': Two input fields showing '27/02/2024' and '00:00:00'.

At the bottom of the dialog, there are three buttons: 'Assistant', 'OK', and 'Annuler'.

Figure 23: Création d'un compte protégé temporaire

Une fois le compte protégé créé, la vue se transforme alors en une liste affichant un compte protégé par ligne.

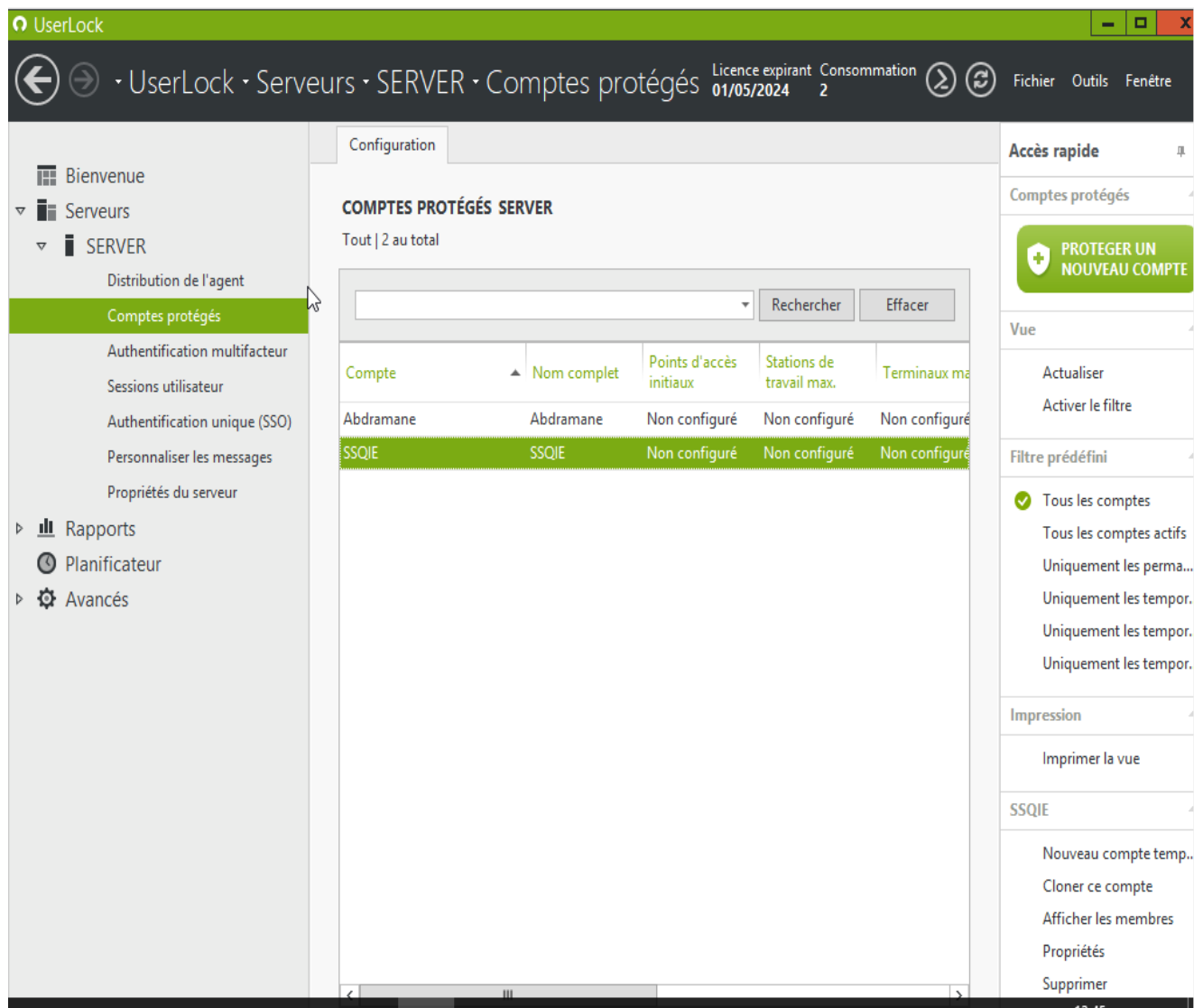


Figure 24: Liste des comptes protégés

A cet instant, aucune règle ni restriction n'est configurée pour ce compte protégé.

Pour éditer les propriétés de ce compte protégé afin de définir des règles de connexion d'accès, des restrictions ou/et des notifications applicables pour chacun des utilisateurs membres de ce groupe, on double-clique sur la ligne.

5.2.9. Configuration des paramètres MFA

Allez dans les paramètres MFA dans la console UserLock.

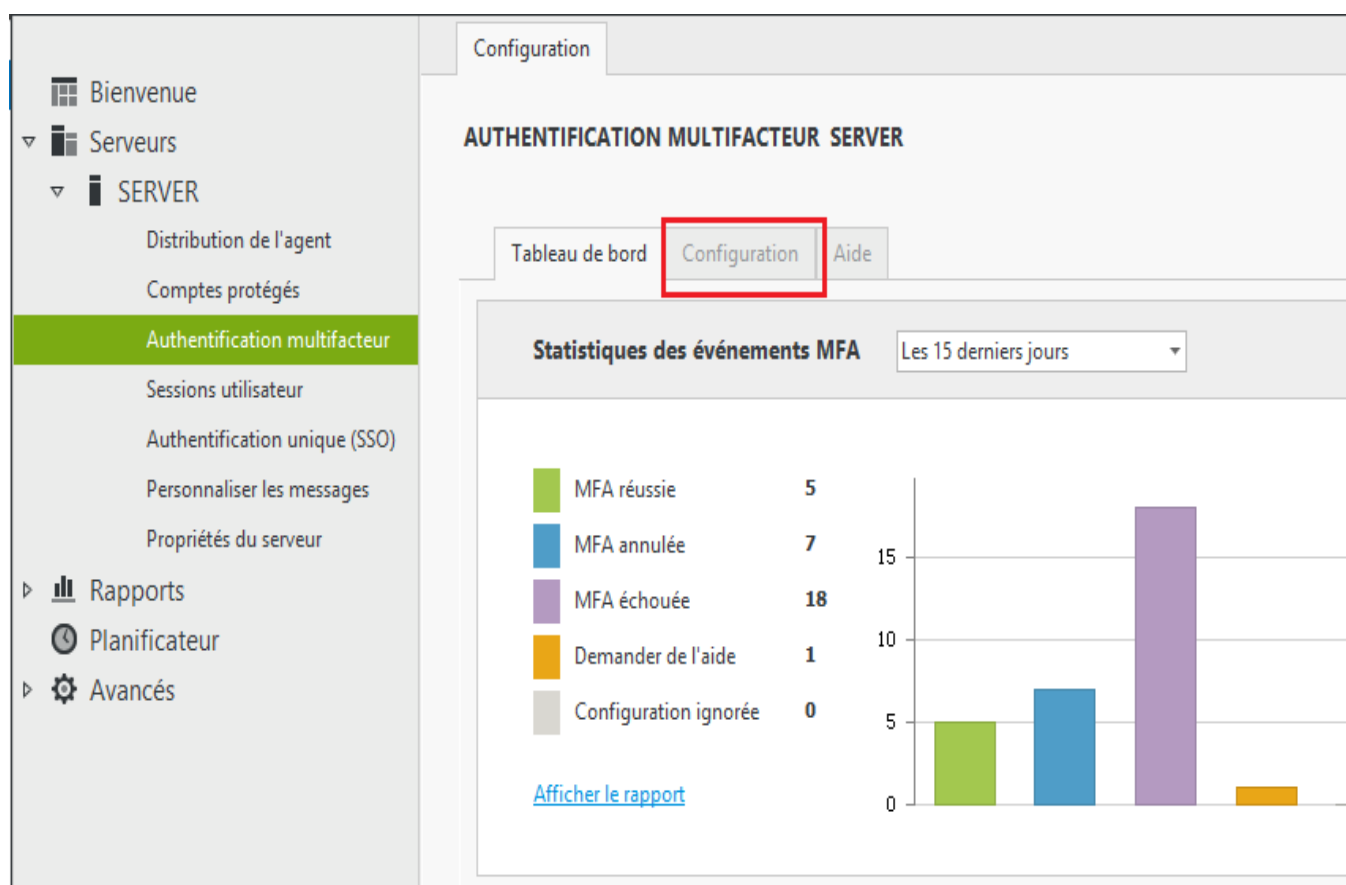


Figure 25: Tableau de bord de l'authentification multi facteur

Demandeur de l'aide : On active cette fonction pour permettre aux utilisateurs de demander de l'aide et de notifier les administrateurs lorsqu'ils ne peuvent pas s'authentifier avec MFA. On met les noms des machines pour recevoir une notification par pop-up, ou on ajoute un ou plusieurs destinataires pour les notifications par e-mail.

Tableau de bord Configuration Aide

Bouton "Demander de l'aide"

Vos utilisateurs peuvent être bloqués par la MFA si par exemple ils n'arrivent pas à configurer leur smartphone ou s'ils "Demander de l'aide" leur permet d'avertir directement leurs administrateurs, qui recevront les notifications par Email désignés.

Activer le bouton "Demander de l'aide"

Envoyer les demandes d'aide par popup
sur la ou les machines suivantes

Envoyer les demandes d'aide par Email
au(x) destinataire(s) suivant(s)

Figure 26: Configuration de “Demander de l’aide”

Méthodes MFA : Par défaut, l'application d'authentification et les jetons USB sont activés. Les notifications push nécessitent une connexion Internet pour notre serveur UserLock, et sont donc désactivées par défaut.

On active les méthodes que nous souhaitons mettre à la disposition des utilisateurs. Toutes les méthodes activées seront proposées aux utilisateurs lors de l'inscription.

Méthodes MFA alternatives : Nous pouvons autoriser ou forcer nos utilisateurs à s'inscrire à deux types de méthodes MFA. Lorsque les utilisateurs s'inscrivent aux notifications push MFA, ils peuvent également accéder à un code TOTP avec l'application UserLock Push. Ce code TOTP leur permet de se connecter au cas où il y aurait un problème de réseau et qu'ils ne pourraient pas recevoir de notifications push.

Les autres méthodes MFA doivent être configurées au moment de l'inscription.

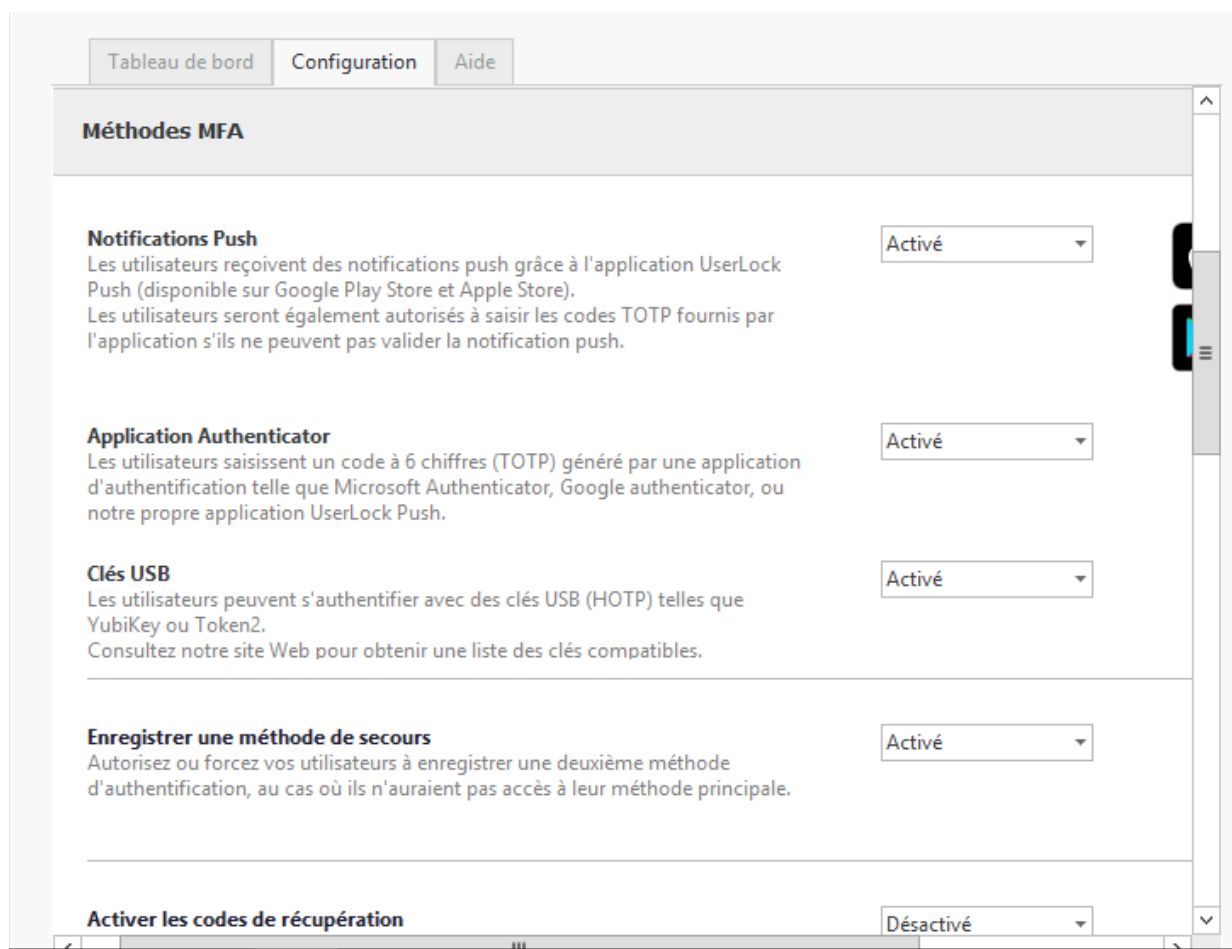


Figure 27: Configuration des méthodes MFA

Codes de récupération : Les codes de récupération sont des codes à usage unique qui peuvent être utilisés pour s'authentifier si l'utilisateur n'a pas accès à son application smartphone ou à son jeton. Ces codes seront présentés à l'utilisateur au moment de l'inscription, et il devra les imprimer et les stocker dans un endroit sûr où il pourra les consulter si nécessaire. Pour générer un nouveau lot de codes, vous devrez réinitialiser la clé MFA de cet utilisateur et il devra se réinscrire.

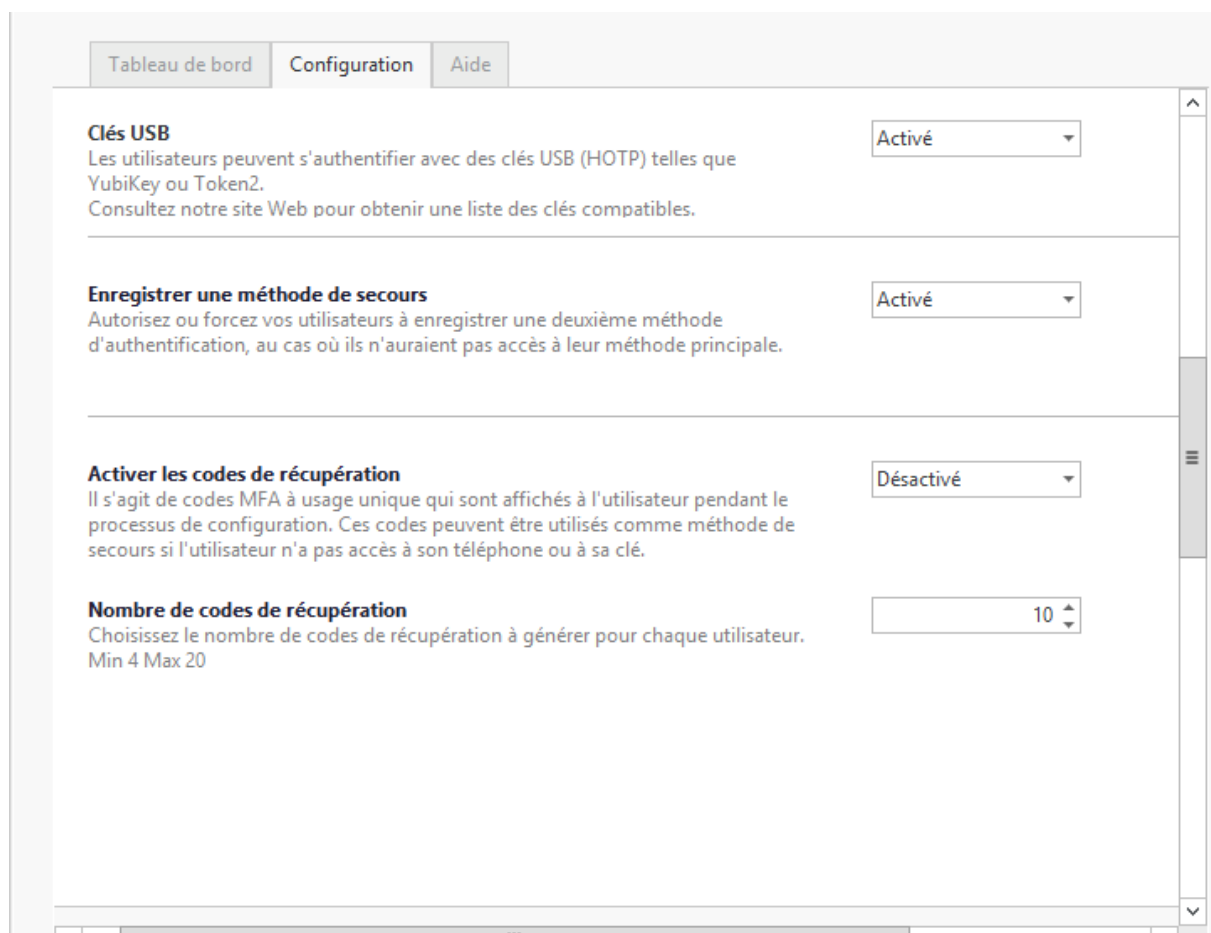


Figure 28: Configuration des codes de récupération

Nous pouvons choisir de fournir 4 à 20 codes par utilisateur.

On clique sur "Appliquer" dans le panneau d'accès rapide pour enregistrer nos paramètres.

5.2.10. Activation de la MFA

Dans la vue Comptes protégés, on double-clique sur un compte protégé pour modifier ses paramètres. On défile la page jusqu'à Authentification multi facteur.

On sélectionne "Activée".

Il y a deux onglets pour les connexions aux postes de travail et aux serveurs (Les sessions IIS et VPN sont considérées comme des connexions serveurs). Cela nous

permet de définir deux polices distinctes pour ces types de connexions. Pour chacune d'elles, nous disposons de 4 options :

- Tous : connexions locales et distantes.
- Distantes : Toute connexion provenant d'une autre machine : RDP, VPN, IIS, etc.
- Provenant de l'extérieur : Toute connexion à distance dont l'adresse IP du client provient de l'extérieur du réseau de l'entreprise.
- Non configuré

On sélectionne la fréquence des invites MFA :

- **Jamais** : ce compte ne sera jamais sollicité pour ces types de connexion.
- **En se connectant pour la première fois à partir d'une nouvelle adresse IP (une fois par adresse)** : lorsqu'un utilisateur se connecte pour la première fois à partir d'une nouvelle adresse IP, il sera demandé de se connecter à MFA. Une fois que cette adresse IP a été enregistrée pour UserLock, il ne sera plus invité à s'authentifier avec MFA.
- **À chaque connexion** : Cela inclut le déverrouillage et la reconnexion à une session à distance.
- **À la première connexion de la journée (une fois par adresse IP)** : Les utilisateurs seront demandés lors de la première connexion de la journée (après minuit) et ne seront à nouveau demandés au cours de la journée que s'ils changent d'adresse IP.
- **Tous les N jours** : Les utilisateurs devront s'authentifier pour chaque adresse IP tous les N jours.
- **Après N jours(s) depuis la dernière connexion depuis cette adresse IP** : Cela fonctionne de la même manière que la deuxième option, sauf que vous pouvez choisir de demander la MFA tous les N jours.

Remarque : les utilisateurs qui se connectent à des sessions à distance avec le même compte depuis une adresse IP qui a déjà été authentifiée avec la MFA ne seront pas sollicités pour ces sessions à distance ultérieures.

Type de session	Types de connexion ?	La MFA sera demandée à ce compte
Tous	Toutes	A chaque connexion
Station de travail	Distant	A chaque connexion
Serveur	Provenant de l'extérieur	A chaque connexion
IIS	Non configuré	A chaque connexion
VPN	Toutes	A chaque connexion
SaaS	Toutes	A chaque connexion

Figure 29: Activation de la MFA pour les comptes protégés

Option Ignorer :

Dans cet onglet, nous pouvons activer un bouton qui permettra aux utilisateurs d'ignorer la configuration MFA jusqu'à une date spécifique. Les utilisateurs seront incités à s'inscrire en fonction de la fréquence que nous avons configurée pour MFA. Une fois cette date passée, ils ne pourront pas se connecter tant qu'ils ne se seront pas inscrits à MFA.

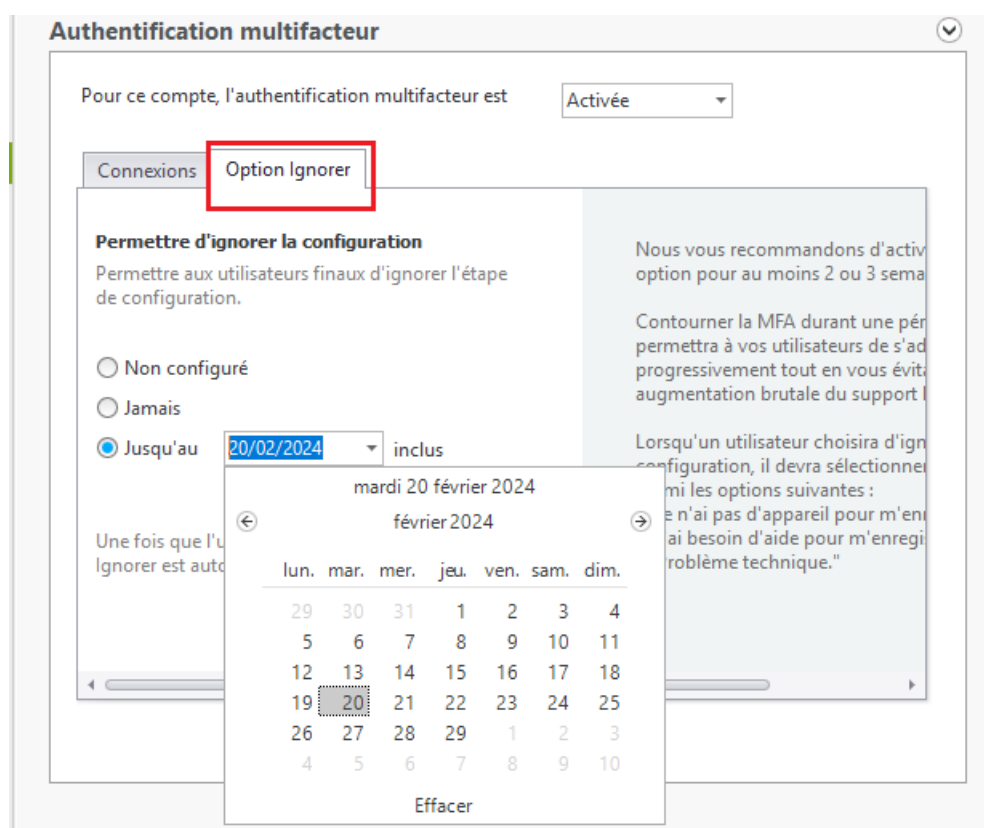


Figure 30: Paramétrage de l'option ignorer

5.3 Tests et Validation

La réalisation de tests approfondis pour garantir le bon fonctionnement du système d'authentification et sa conformité aux normes de sécurité.

Indépendamment de l'application que nous choisissons, assurons-nous que la date et l'heure du smartphone des utilisateurs finaux est correcte (il est recommandé de régler la date et l'heure automatiquement), sinon les codes générés par l'application ne peuvent pas être validés.

Pour la première connexion MFA d'un utilisateur, cet utilisateur peut avoir besoin d'aide pour la configuration.

- Une fois que la MFA est activée pour un compte d'utilisateur, lors de sa prochaine connexion, une boîte de dialogue avec un QR code sera affichée :

Authentification Multifacteur

Configuration de l'authentification multifacteur

Votre compte est protégé par MFA. Suivez les étapes pour configurer MFA avec votre smartphone. Lorsque vous choisissez une application d'authentification, une option populaire est Google Authenticator (gratuit sur Android et iOS).

- Télécharger une application d'authentification**

Veuillez installer une application d'authentification sur votre périphérique. Par exemple, vous pouvez chercher 'authenticator' dans votre Application Store.
- Scanner le QR Code**

Veuillez ouvrir l'application téléchargée précédemment afin de scanner le code-barres ci-dessous.



Si vous ne parvenez pas à scanner le code-barres, vous pouvez entrer la clé ci-dessous manuellement dans l'application

Q2JAKK4GL7NCVNYI
- Valider le code d'authentification**

Veuillez entrer le code à 6 chiffres affiché par votre application

Valider et continuer

Passer (encore 21 jours)

Demander de l'aide

Annuler

Comment installer une application d'authentification

Si vous n'avez pas d'application d'authentification sur votre périphérique, veuillez vous rendre sur le Google Play Store (systèmes Android) ou sur l'App Store (iPhones) pour en installer une.

Veuillez synchroniser la date et l'heure automatiquement sur votre périphérique. Dans le cas d'une configuration manuelle, les codes générés pourraient être erronés ce qui provoquerait une erreur lors de l'ouverture de la session.

Si vous n'avez pas votre téléphone, cliquez sur le bouton "Demander de l'aide" pour prévenir votre support technique.

Vous pouvez également cliquer sur 'Passer' pour configurer votre compte plus tard.

Figure 31: Configuration de l'authentification multifacteur

- Lorsque cette boîte de dialogue apparaît, l'utilisateur doit ouvrir l'application d'authentification sur son smartphone, puis scanner le code-barres. Par exemple avec Google Authenticator :

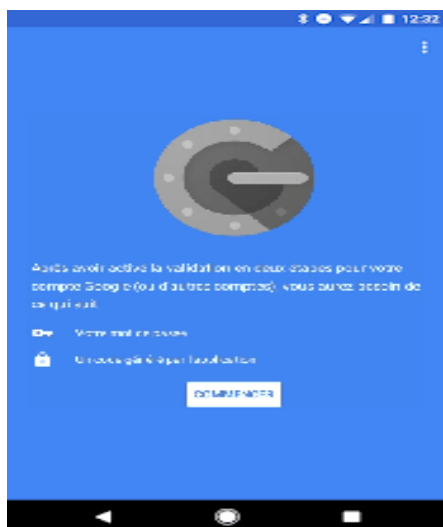


Figure 32: Google authenticator

- On clique sur « Commencer »
- Dans l'étape « Ajouter un compte », choisissez « Scanner un code-barres » (ou « Saisir une clé fournie » si vous préférez) :

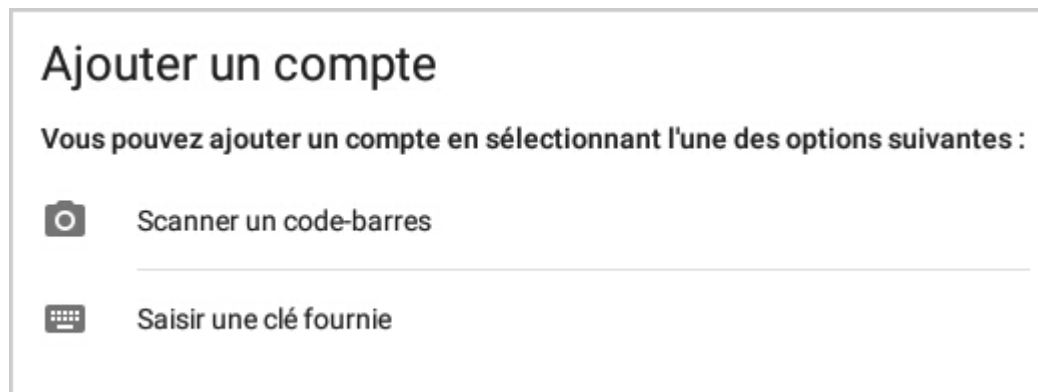


Figure 33: Ajouter un compte

- Le code MFA est maintenant affiché :

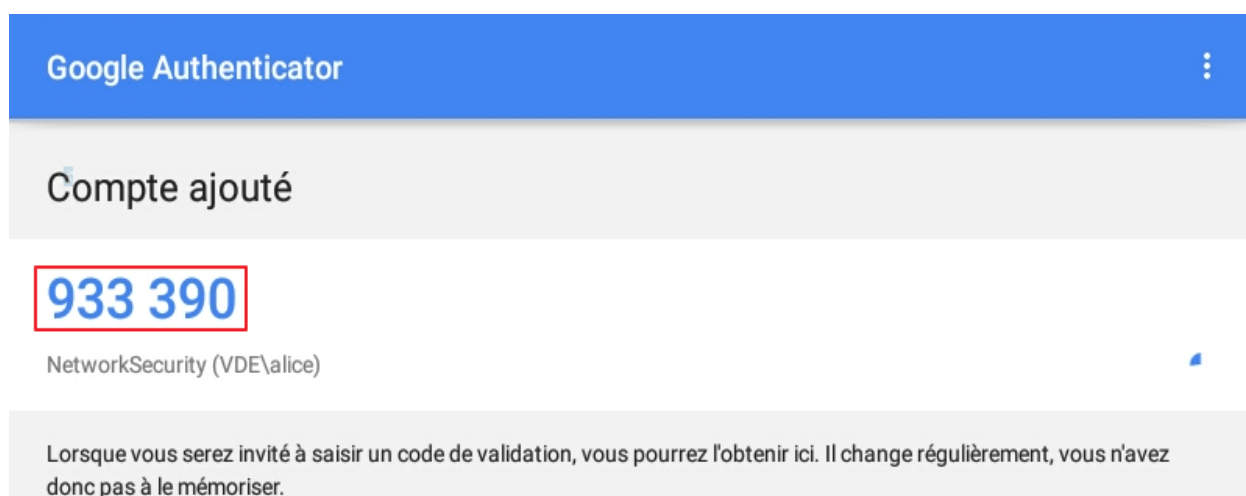
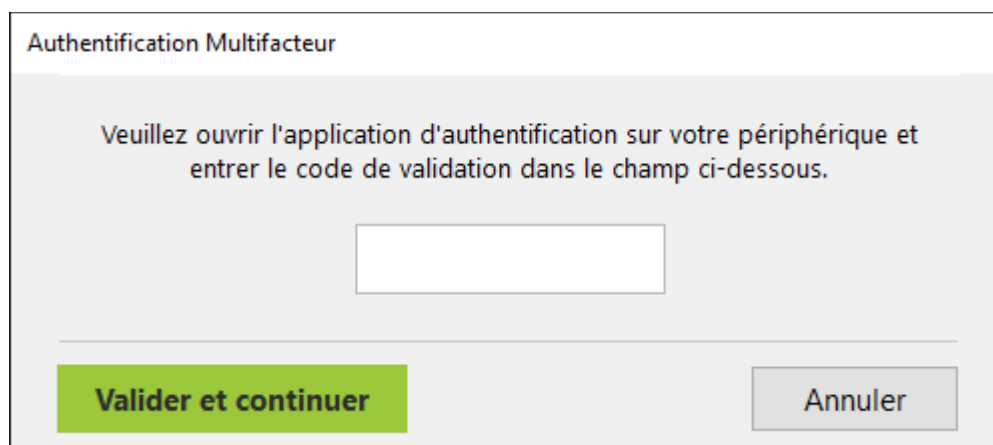


Figure 34: Code MFA

- On remplit le code MFA dans le champ de la boîte de dialogue, puis on clique sur « Valider et continuer ».

Une fois correctement configuré, la boîte de dialogue suivante sera proposée à l'utilisateur pour toutes les connexions nécessitant MFA.



Authentification Multifacteur

Veuillez ouvrir l'application d'authentification sur votre périphérique et entrer le code de validation dans le champ ci-dessous.

Valider et continuer Annuler

Figure 35: Saisi de code

5.4 Bilan

5.4.1 Points des réalisations

N'ayant aucun serveur disponible au moment du déploiement, le système d'authentification 2FA a été dès le départ déployé sur une machine virtuelle fonctionnant sous Windows.

Nous pouvons affirmer que la solution d'authentification à 2FA a été bien étudiée. L'installation a été bien faite et la solution répond aux attentes de notre structure d'accueil. Cependant il faut noter qu'un retard a été accusé dans la réalisation du projet. Le prochain point évoque la question de cet écart.

5.4.2 Explication des écarts

Il existe un écart très remarquable entre le planning prévisionnel et le planning réel lors de l'implémentation de la solution. En effet le projet devant finir fin novembre 2023 se voit finir jusqu'en début mars 2024 ce qui a pour conséquence le bouleversement total sur le planning prévisionnel. Ce décalage temporel se justifie par :

- ✓ le changement de thème ;

- ✓ l'étude des méthodes d'authentifications et la maîtrise des protocoles, outils et logiciels d'authentifications ont pris plus de temps que prévu ;
- ✓ la participation à certaines activités de l'entreprise ;
- ✓ l'absence d'un environnement de test.

Le planning réel est représenté dans la **figure 31** à l'aide d'un diagramme de GANTT :

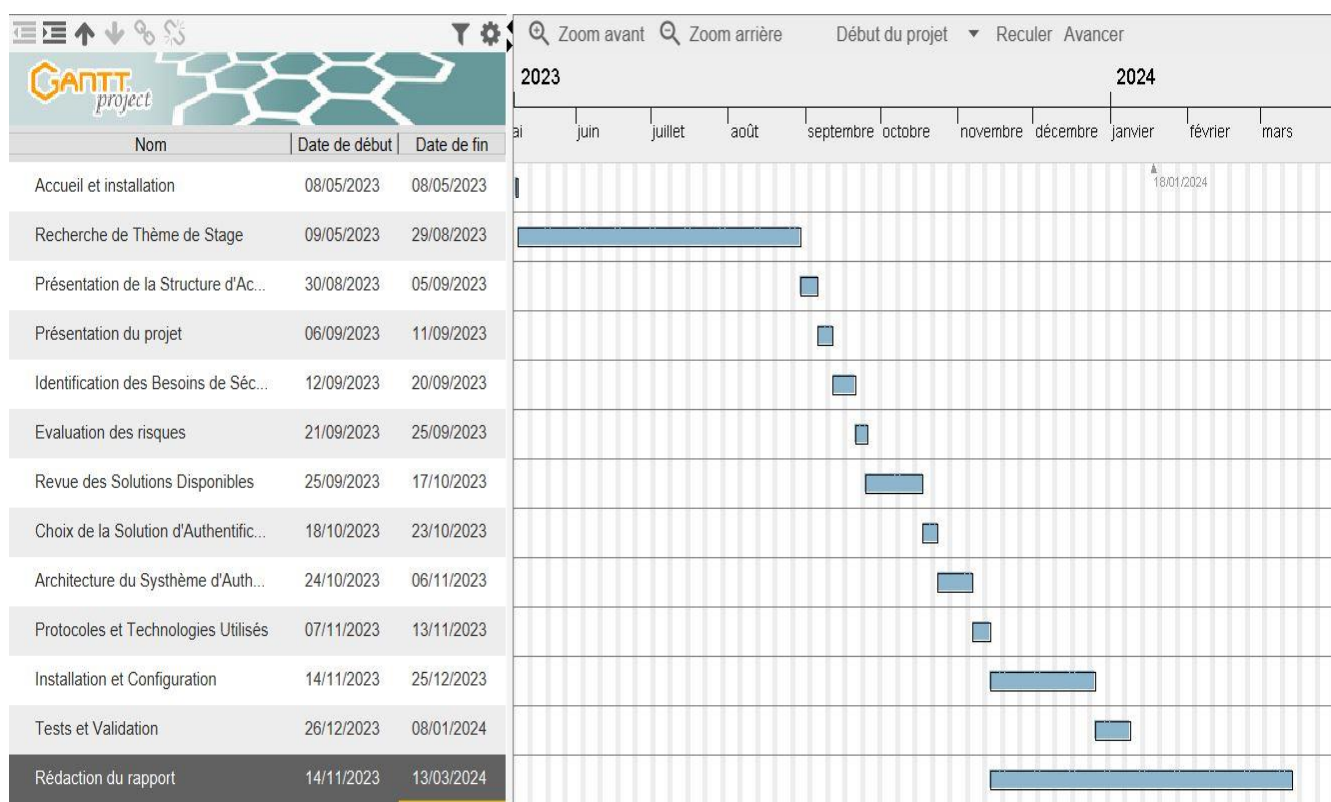


Figure 36: Diagramme réel

5.5 Conclusion

Dans ce chapitre nous nous sommes penchés sur l'aspect pratique du projet, en détaillant les étapes de sa mise en place et de son utilisation. Ainsi avec l'apport du logiciel UserLock nous avons pu montrer l'importance de la mise en place d'un système 2FA, qui est principalement, le renforcement de la sécurité des comptes utilisateurs, mais aussi la réduction des risques de compromission du système ou des ressources. Et nous avons estimé les coûts de sa réalisation.

CONCLUSION GENERALE

Le présent rapport fait le bilan de notre stage de fin de cycle en licence d'informatique dont le thème est : « **Étude et mise en place d'un système d'authentification dans le réseau IP du Centre MURAZ** ». Ce thème représente une étape cruciale dans l'amélioration de la sécurité et de la confidentialité des données médicales au sein de l'institution. Au cours de cette recherche, nous avons examiné en détail les besoins spécifiques du Centre Muraz en matière de sécurité informatique, ainsi que les défis et les enjeux associés à la protection des données sensibles dans un environnement médical.

La mise en place du système d'authentification a permis de renforcer la protection des informations confidentielles en restreignant l'accès aux utilisateurs autorisés uniquement. Grâce à des méthodes d'authentification robustes telles que l'authentification à deux facteurs et la gestion centralisée des identités, nous avons créé un environnement sécurisé où seules les personnes habilitées peuvent accéder aux données médicales sensibles. Cependant, il est important de reconnaître que la sécurité informatique est un processus continu et évolutif. Par conséquent, il est essentiel de maintenir et de mettre à jour régulièrement le système d'authentification pour faire face aux nouvelles menaces et aux évolutions technologiques. De plus, une sensibilisation et une formation continues des utilisateurs sont indispensables pour garantir une utilisation sûre et responsable des ressources informatiques.

Pour garantir un niveau optimal de sécurité informatique, plusieurs mesures essentielles doivent être prises. Tout d'abord, il est primordial d'organiser des sessions de sensibilisation régulières pour le personnel, afin de les informer sur les meilleures pratiques en matière de sécurité informatique, les risques potentiels et les

mesures de prévention. En parallèle, la mise en place d'un système de surveillance continue permet de détecter rapidement les menaces de sécurité émergentes et les activités suspectes sur le réseau, assurant ainsi une réponse proactive aux incidents. De plus, l'organisation devrait planifier et réaliser des audits de sécurité périodiques pour évaluer l'efficacité des mesures en place, identifier les vulnérabilités et proposer des recommandations pour les corriger. Enfin, investir dans la formation continue du personnel en matière de sécurité informatique garantit que l'équipe est toujours au fait des dernières menaces et des meilleures pratiques de sécurité, renforçant ainsi la posture globale de sécurité de l'organisation.

Comme bilan de fin de stage, sur le plan intellectuel nous avons approfondi nos connaissances sur la sécurité informatique. À l'instar de cela, nous pouvons dire que ce stage de fin d'étude de licence fut une première véritable expérience en entreprise car la formation théorique reçue durant le cursus universitaire a été complétée par les formations pratiques reçues au Centre MURAZ.

REFERENCES

- [1] : <https://u-auben.com/>, consulté le 29/02/2024;
- [2] : [https://www.google.com/search?q=Authentification%](https://www.google.com/search?q=Authentification%20), consulté le 19/12/2023;
- [3] : <https://chat.openai.com/c/8abaa08a-443d-4634-8d0d-bfa9bb8cb107>, consulté le 19/12/2023;
- [4] : <https://www.sailpoint.com/fr/identity-library/authentication-methods-used-for-network-security/>, consulté le 19/12/2024;
- [5] : [https://www.google.com/search?q=Sch%C3%A9ma+de+l%27Authentification+%C3%A0+deux+facteurs+\(2FA\)](https://www.google.com/search?q=Sch%C3%A9ma+de+l%27Authentification+%C3%A0+deux+facteurs+(2FA)), consulté le 19/12/2024;
- [6] : <https://next.ink/17345/96167-u2f-double-authentification-par-clef-usb-se-repand-et-debarque-dans-dropbox/>, consulté le 19/12/2023;
- [7] : <https://www.isdecisions.fr/logiciels/userlock/aide/getting-started-guide/index.htm>, consulté le 14/02/2024;
- [8] : https://www.isdecisions.fr/logiciels/userlock/aide/agents/desktop_agent/agent.htm;
- [9] : <https://www.isdecisions.fr/logiciels/userlock/aide/requirement.htm>;

- [10] : <https://www.microsoft.com/fr-fr/d/licence-dacces-client-windows-server-2019-standard/dg7gmgf0dvss>;
- [11] : <https://www.isdecisions.fr/logiciels/userlock/tarifs.htm>;
- [12] : Abdramane, Z. (s.d.);
- [13] : Formation, « Sensibilisation aux enjeux de la sécurité numérique et aux cybermenaces ».
- Par Dr Beman H. KAMAGATE, Enseignant-Chercheur. Bobo Dioulasso/ Centre MURAZ.;
- [14] : <https://www.isdecisions.fr/logiciels/userlock/aide/use-cases/multi-factor-authentication.htm>, consulté le 14/02/2024;
- [15] : <https://www.isdecisions.fr/telecharger/userlock.htm>, consulté le 14/02/2024;
- [16] : Mamadou, D. (11 Mai 2017). *Etude de la mise en place d'une solution de contrôle d'accès au réseau à travers le protocole 802.1X. Page 10*. Paris;
- [17] : Massinissa, M. M. (2014/2015). « *Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP* », Page 116-128. . RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE: UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU.