PAGE DE GARDE DU DOSSIER PROFESSIONNEL

BREVET DE TECHNICIEN SUPÉRIEUR SERVICES INFORMATIQUES AUX ORGANISATIONS

Session 2026

DOSSIER PROFESSIONNEL

NOM : VIAUD

Prénom : Julien

Établissement de formation (sur un seul des deux exemplaires du dossier)

Visa du représentant de l'équipe pédagogique attestant la réalité des activités professionnelles décrites dans le dossier (sur un seul des deux exemplaires du dossier) :

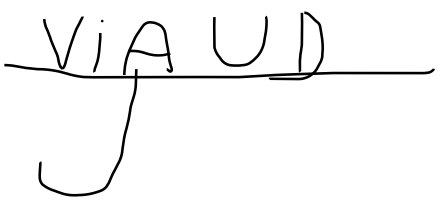
Nom et qualité du signataire	Date	Signature
BOLLIN Antonin Formateur SIO SISR	23/04/2026	

Attestation sur l'honneur pour les candidats individuels (sur un seul des deux exemplaires du dossier) :

Je soussigné(e), VIAUD , Julien , certifie que les activités décrites ainsi que les différentes informations reproduites dans ce dossier reflètent les activités professionnelles que j'ai personnellement réalisées au cours de ma formation.

Fait à La Roche sur Yon
Date 28/04/2026

Signature



SITE DE LA ROCHE SUR YON
/ ATLANTIC INDUSTRIE

GROUPE ATLANTIC

ATTESTATION PROFESSIONNELLE

Je soussignée, Sophie PAULAY, agissant en qualité de Responsable RH unité d'Atlantic Industrie, Rue Monge, Zone Acti'Nord à La Roche Sur Yon (85 000), certifie que Monsieur VIAUD Julien, né le 29/03/2006, est salarié alternant au sein de l'entreprise depuis le 19/08/2024, et ce en contrat à durée déterminée.

Il n'est actuellement ni en préavis, ni en procédure de licenciement.

Pour faire valoir ce que de droit,

Fait à LA ROCHE SUR YON,
Le lundi 27 avril 2026

Sophie PAULAY
Responsable Ressources Humaines Unité

ATLANTIC INDUSTRIE
S.A.S au capital de 2.631.000 €
Rue Monge ZA Acti'Nord Monge
85000 LA ROCHE SUR YON
SIRET 352 529 499 00019 - APE 297A

ATLANTIC INDUSTRIE – S.A.S. au capital de 2 631 000 € - Siège social et Usine : Rue Monge, ZA Acti'Nord - Monge, 85000 LA ROCHE SUR YON
Tél. (33) 2 51 44 34 34 - Fax (33) 2 51 36 35 96 - Fax chauffage (33) 2 51 37 37 73 - Fax eau chaude (33) 2 51 46 19 63 - Fax électronique (33) 2 51 05 25 68 - Site internet : groupe-atlantic.com
Services administratifs : 44, Boulevard des Etats-Unis - 85000 LA ROCHE SUR YON - Adresse postale : BP 65 – 85002 La Roche-sur-Yon CEDEX

Table des matières

Tableau de synthèse 4

Ma présentation 5

Remerciement 6

Présentation du groupe et de l'entreprise 7

MISSION 1 : Création de compte 16

- Mise en situation 17
- Ma mission 18

MISSION 2 : Intégration d'un macOS dans l'AD 26

- Mise en situation 27
- Ma mission 28

Conclusion 48

ANNEXES 49

- SSID - GAOFFICEOSX 50
- APPLE MAC _ Linux Management 54

Tableau de synthèse

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS | **SESSION 2026**

Tableau de synthèse des réalisations professionnelles

NOM et prénom : VIAUD Julien | **N° candidat : 2543700461**

Centre de formation : Fab'Academy - La Roche sur Yon | **Option :** ☑ SISR ☐ SLAM

Adresse URL du portfolio :https://julien.viaud.formation-esiac.fr/

Compétences mises en œuvre / *Réalisations professionnelles (intitulé et liste des documents et productions associés)*	Période (sous la forme du JJ/MM/AA au JJ/MM/AA)	Gérer le patrimoine informatique	Répondre aux incidents et aux demandes d'assistance et d'évolution	Développer la présence en ligne de l'organisation	Travailler en mode projet	Mettre à disposition des utilisateurs un service informatique	Organiser son développement professionnel
		▸ Recenser et identifier les ressources numériques ▸ Exploiter des référentiels, normes et standards adoptés par le prestataire informatique ▸ Mettre en place et vérifier les niveaux d'habilitation associés à un service ▸ Vérifier les conditions de la continuité d'un service informatique ▸ Gérer des sauvegardes ▸ Vérifier le respect des règles d'utilisation des ressources numériques	▸ Collecter, suivre et orienter des demandes ▸ Traiter des demandes concernant les services réseau et système, applicatifs ▸ Traiter des demandes concernant les applications	▸ Participer à la valorisation de l'image de l'organisation sur les médias numériques en tenant compte du cadre juridique et des enjeux économiques ▸ Référencer les services en ligne de l'organisation et mesurer leur visibilité. ▸ Participer à l'évolution d'un site Web exploitant les données de l'organisation.	▸ Analyser les objectifs et les modalités d'organisation d'un projet ▸ Planifier les activités ▸ Évaluer les indicateurs de suivi d'un projet et analyser les écarts	▸ Réaliser les tests d'intégration et d'acceptation d'un service ▸ Déployer un service ▸ Accompagner les utilisateurs dans la mise en place d'un service	▸ Mettre en place son environnement d'apprentissage personnel ▸ Mettre en œuvre des outils et stratégies de veille informationnelle ▸ Gérer son identité professionnelle ▸ Développer son projet professionnel
Réalisation en cours de formation							
Mise en place d'un GLPI (Serveur Linux, MariaDB, Apache)	27/11/2025 au 03/11/2025	x	x		x	x	x
Création d'une entreprise pédagogique	25/08/2025 au 05/09/2025				x	x	x
Mise en place de serveurs Web pour l'entreprise	22/09/2025 au 03/10/2025			x			x
Configuration de switch	27/11/2025 au 03/11/2025	x					x
Mise en place d'un Proxmox pour l'entreprise	25/08/2025 au 05/09/2025	x			x		x
Portofolio	24/11/2025 au 27/03/2026			x			x
Réalisations en milieu professionnel en cours de première année							
Création des Utilisateur + déploiement de PC + téléphone mobile	19/08/2024 au 08/08/2025	x	x		x		
Gestion des Ticket GLPI	19/08/2024 au 08/08/2025		x				
Migration Windows 11	19/08/2024 au 08/08/2025		x	x		x	
Réalisations en milieu professionnel en cours de seconde année							
Configuration PC Linux	08/09/2025 au 17/04/2026	x	x			x	x
Configuration PC macOS	08/09/2025 au 17/04/2026	x	x			x	x
Création des Utilisateur + déploiement de PC + téléphone mobile	08/09/2025 au 17/04/2026	x	x		x		
Gestion des Ticket GLPI	08/09/2025 au 17/04/2026		x				
Migration Windows 11	08/09/2025 au 17/04/2026		x	x		x	

Ma présentation

Je me présente, Julien VIAUD, issu d'un bac professionnel Système Numérique. J'ai choisi de poursuivre mes études en BTS SIO à l'UIMM Fab'academy et en alternance dans l'entreprise Atlantic Industrie, appartenant au Groupe Atlantic, en tant que référent informatique.

Ce dossier professionnel U5 s'inscrit dans le cadre de ma formation en BTS SIO option SISR (Solutions d'Infrastructure, Systèmes et Réseaux) à l'UIMM Fab'Academy. Cette option a pour objectif de me préparer aux métiers de l'administration système, des réseaux et de la sécurité informatique. Les missions présentées dans ce dossier illustrent concrètement ces compétences : la gestion des comptes utilisateurs relève de la gestion des accès et des droits (un pilier de la sécurité des systèmes d'information), tandis que l'intégration de postes macOS dans l'Active Directory touche directement à la sécurisation du domaine et à la conformité du parc informatique.

Dans ce document, je vous présenterai le Groupe Atlantic et Atlantic Industrie, où j'ai effectué mon alternance en tant que référent informatique, ainsi que mes missions et réalisations au sein de celle-ci.

Remerciement

Je souhaite adresser mes remerciements aux personnes qui m'ont apporté leur aide et qui ont contribué à l'élaboration de ce dossier ainsi qu'à la réussite de ma formation.

Je tiens à remercier Aurélien CREPEAU, qui, en tant que responsable informatique, m'a accueilli dans son équipe. Je remercie également mon tuteur Virgile ROCHETEAU pour son accompagnement, sa disponibilité et son expertise, ainsi que l'ensemble de l'équipe informatique de mon site.

Merci à l'école, à l'équipe pédagogique, aux formateurs et à mon formateur principal Mr. BOLLIN pour son accompagnement tout au long de l'année.

Enfin, je remercie mes proches, et notamment mes parents, pour leur soutien tout au long de cette année et leur contribution en tant que relecteurs de ce dossier.

Présentation du groupe et de l’entreprise

Le Groupe Atlantic a été fondé en 1968 par Paul Radat et Pierre Lamoure à La Roche-sur-Yon en Vendée (85).

Le groupe a connu une croissance significative depuis sa fondation en 1968, passant d'une entreprise spécialisée dans les chauffe-eaux électriques à un leader européen dans le domaine du confort thermique et sanitaire, avec un fort engagement envers l'innovation et le développement durable.

Logo actuel du Groupe Atlantic

Aujourd'hui, le groupe continue d'évoluer et de se positionner en tant que leader dans son secteur, en anticipant les tendances du marché et en répondant aux besoins en constante évolution des consommateurs.

L’engagement du Groupe Atlantic en faveur du confort, de la performance énergétique et du développement durable en fait un partenaire privilégié dans la réalisation de projets de chauffage, de climatisation et de production d'eau chaude, tant pour les bâtiments résidentiels que pour les établissements commerciaux et industriels.

Le Groupe Atlantic a établi sa présence à l'échelle mondiale en s'implantant dans plusieurs pays. Ses sites de production, bureaux et centres de recherche et développement sont stratégiquement localisés pour mieux servir ses clients à travers le monde.

Cette expansion internationale s’est principalement déployée à partir des années 2000 et a pris de l’ampleur au cours de la décennie 2010, en particulier sur les marchés émergents tels que l’Inde, la Géorgie et la Turquie.

Présence du Groupe Atlantic sur le globe

Le Groupe Atlantic adopte une structure organisationnelle stratégique, se composant de plusieurs divisions essentielles telles que le chauffage, le traitement de l'air, la plomberie et les énergies renouvelables.

Par exemple, le site d'Atlantic Industrie à La Roche-sur-Yon (85), où je poursuis mon apprentissage, est structuré en trois entités de production autonomes + une plateforme logistique : E2C* (spécialisée dans la fabrication de cartes électroniques), CEL (spécialisée dans la production de chauffage), CHOD (spécialisée dans la production de chauffe-eau) et LPF (plateforme logistique).

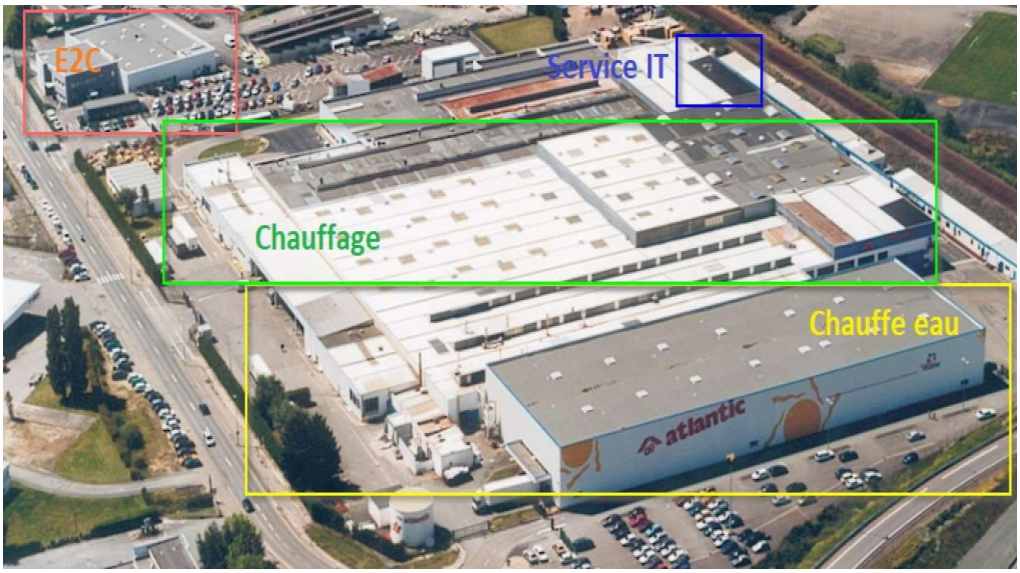


Photo aérienne du site Atlantic Industrie

Chacune des trois entités de production est supervisée par sept services techniques spécifiques (production, processus, qualité, logistique, maintenance, recherche et développement, et achats).

Il y a également six services transversaux aux trois unités de production et à la plateforme logistique, à savoir le SATC*, l'industrialisation, les ressources humaines, les infrastructures, la QSE* et l'IT où je suis en alternance.

Le Groupe Atlantic compte environ 13 000 collaborateurs répartis à travers le monde. Cette équipe diversifiée et hautement qualifiée constitue un pilier essentiel de la réussite et de la croissance continue du groupe.

Le Groupe Atlantic propose une large gamme de produits et de services dans le domaine du confort thermique, y compris des systèmes de chauffage, des solutions de traitement de l'air, des produits de plomberie et des technologies innovantes pour les énergies renouvelables. Le groupe fabrique par an approximativement 10 millions d’appareils.

Exemple d’appareils produits par le Groupe Atlantic

Le groupe a réalisé un chiffre d'affaires de 3,2 milliards d’euros net au cours de l'année 2022. Cette performance financière solide témoigne de la confiance des clients dans la qualité des produits et des services.

Le groupe compte parmi ses clients des particuliers, des entreprises, des institutions publiques ainsi que des partenaires dans le secteur de la construction et de la rénovation.

Dans un marché concurrentiel, le Groupe Atlantic se distingue par son innovation constante, sa qualité de fabrication et son service client. Il maintient sa position de leader sur le marché en rivalisant avec les meilleurs acteurs de l'industrie.

Voici une liste des principales marques faisant partie du Groupe Atlantic :

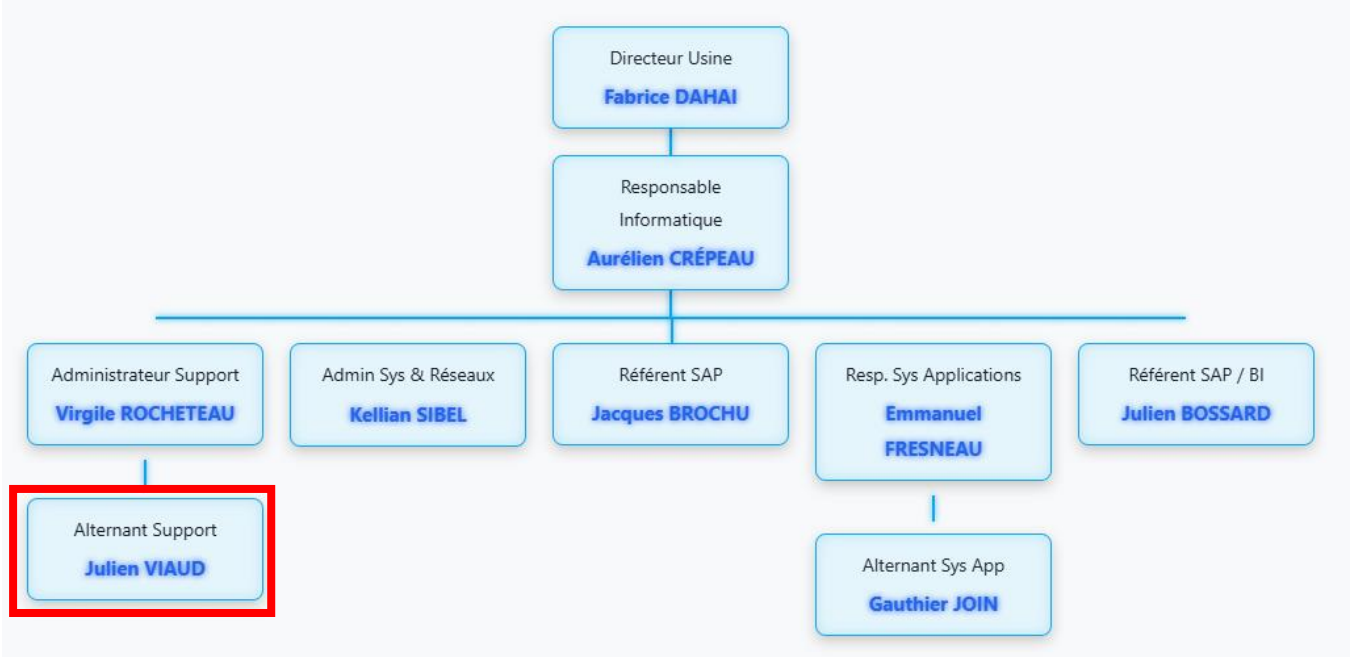
Les principaux concurrents sont Daikin Industries (Japon), Bosch Thermo technologie (Allemagne) ou encore Viessmann (Allemagne).

Le Groupe Atlantic s'engage à fournir des solutions de confort thermique de haute qualité, respectueuses de l'environnement et économiquement viables. Son processus de production intègre les dernières technologies et les meilleures pratiques pour garantir la fiabilité et la performance des produits.

Le processus de production du Groupe Atlantic repose sur des normes strictes de qualité et de sécurité. De la conception initiale à la fabrication et à la distribution, chaque étape est minutieusement planifiée et exécutée pour répondre aux besoins et aux attentes des clients.

Comme dit précédemment, j'ai rejoint l'équipe IT du site Atlantic Industrie de la Roche-sur-Yon (85).

Voici l'organigramme de l'équipe :



Le service informatique du site Atlantic Industrie est chargé d'assurer le bon fonctionnement des systèmes informatiques liés à la production.

Cela comprend la gestion des logiciels et des équipements utilisés dans le processus de fabrication, ainsi que la maintenance régulière pour minimiser les interruptions de production.

De plus, le service informatique veille à la sécurité des données de production en mettant en place des mesures de protection contre les cybermenaces. Il peut également jouer un rôle dans l'intégration de nouvelles technologies visant à améliorer l'efficacité et la qualité des opérations.

En outre, il assure la formation du personnel à l'utilisation des systèmes informatiques spécifiques à la production et collabore avec d'autres départements pour garantir une intégration harmonieuse des systèmes informatiques dans l'ensemble des processus de l'entreprise.

Le service est de plus placé sous l'autorité de la DSI du Groupe Atlantic, située à La Roche sur-Yon (85). Nous avons des contacts quotidiens avec la DSI, notamment parce qu'ils gèrent la cybersécurité de tous les sites du Groupe Atlantic.

Concernant le support utilisateur, nous sommes également en contact avec eux : lorsqu'un utilisateur de notre site rencontre un problème, il se tourne d'abord vers nous, et nous déterminons ensuite si le problème peut être résolu par notre équipe locale ou s'il doit être transmis à la DSI (niveau 2, puis niveau 3, puis support externe type Microsoft).

MISSION 1 : Création de compte

Mise en situation

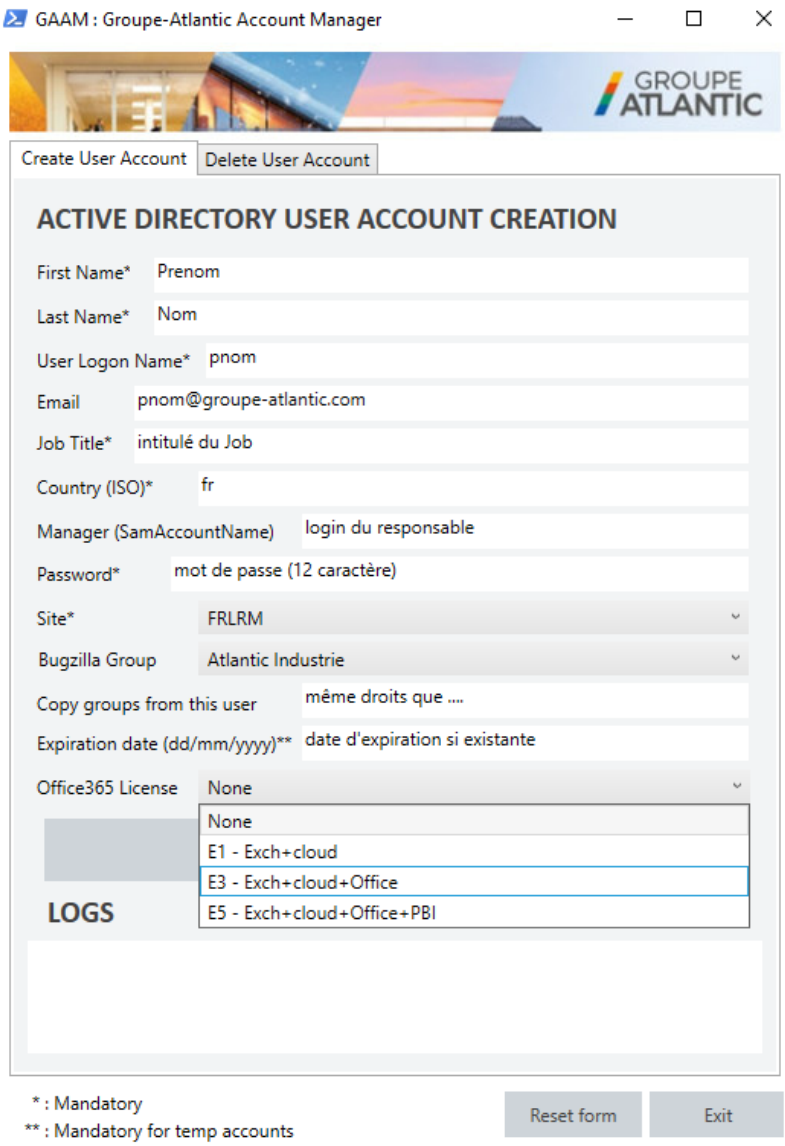
Sur notre outil GLPI (Gestion Libre de Parc Informatique), nous recevons régulièrement des demandes de création de compte pour tout type de contrats (CDI, CDD, alternance, intérimaire, stage). Ces demandes sont généralement émises par les responsables de service ou le département des ressources humaines, à l'occasion de l'arrivée d'un nouvel employé sur site.

À la réception de cette demande, nous créons les comptes utilisateurs en suivant une procédure définie par le service informatique, garantissant la cohérence et la sécurité des accès sur l'ensemble du parc. L'enjeu de cette procédure est d'assurer que chaque utilisateur dispose des bons accès dès son premier jour, sans surplus de droits (principe du moindre privilège), et que toutes les informations soient correctement renseignées dans l'Active Directory du Groupe Atlantic.

Ma mission

Étape 1 – Création du compte dans GAMM-OP :

GAMM-OP est l'outil interne du Groupe Atlantic permettant d'initialiser les comptes utilisateurs sur l'infrastructure Microsoft. On y renseigne les informations identitaires du collaborateur (nom, prénom, service, type de contrat) ainsi que le type de licence Microsoft 365 à attribuer. La licence E3 est attribuée par défaut : elle inclut le client mail Outlook et les applications Office 365 en version installable et web. Dans certains cas spécifiques (intérimaires, stagiaires courts), la licence E1 est utilisée, donnant uniquement accès aux versions en ligne d'Office. Le choix de la licence a un impact direct sur les coûts et sur les droits de l'utilisateur. Après validation, un brouillon est préparé avec les identifiants générés (login Windows et adresse mail), qui seront ensuite transmis au responsable du nouveau collaborateur.



LICENCE E3 (SAUF CAS PARTICULIERS : E3 = MAIL + O365 APPLI/ONLINE, E1 = MAIL + O365 ONLINE)

Penser à remplir ce mail dans un brouillon pour ne pas perdre les informations importantes

Voici les identifiants Windows et Outlook pour : Prénom Nom

Login : pnom

Mot de passe : ……

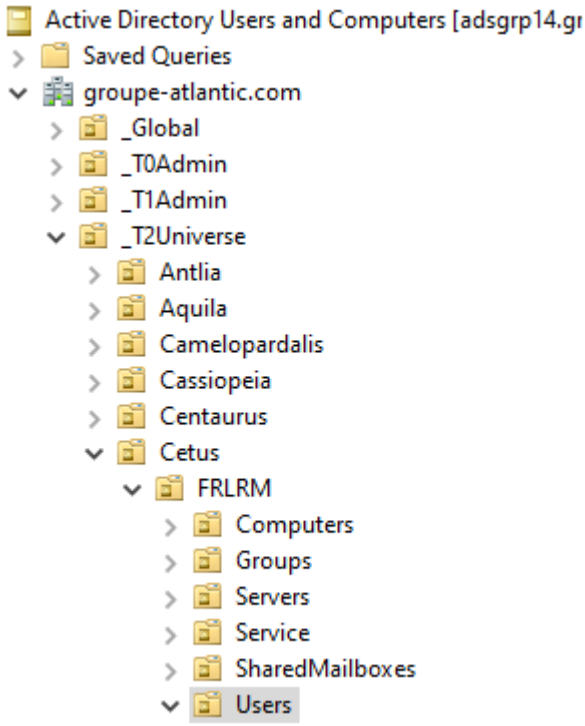
Adresse : pnom@groupe-atlantic.com

Merci de lui transmettre ces informations.

Si des accès complémentaires sont nécessaires, vous pouvez revenir vers nous.

Étape 2 –

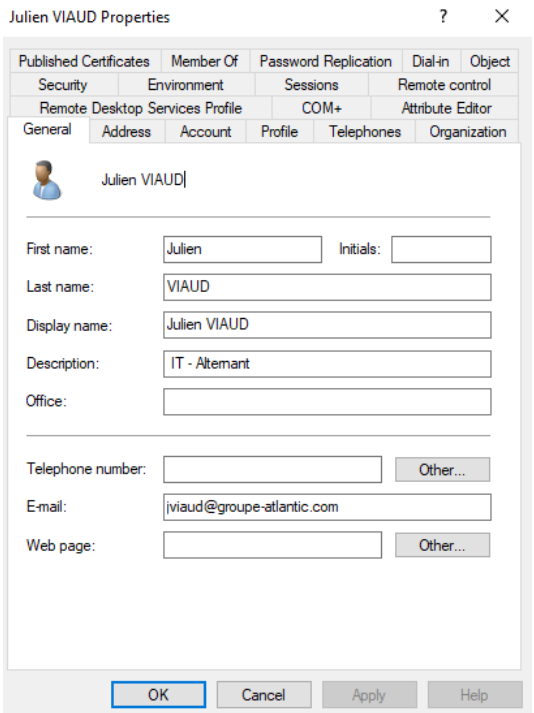
Localisation et déplacement dans l'Active Directory : Une fois le compte créé via GAMM-OP, il apparaît dans un conteneur générique de l'AD (Active Directory). Il faut le retrouver dans la console Active Directory Users and Computers (ADUC) puis le déplacer dans la bonne Unité d'Organisation (OU).

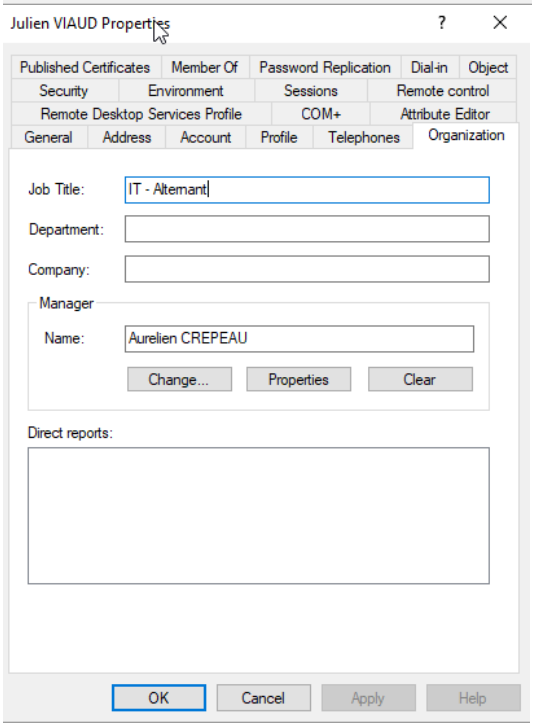


Étape 3 –

Placement dans la bonne OU : Chaque service de l'entreprise correspond à une Unité d'Organisation (OU) spécifique dans l'AD. Ce classement est essentiel : les Stratégies de Groupe (GPO) appliquées à chaque OU définissent les droits, les lecteurs réseau mappés et les logiciels installés automatiquement. Un utilisateur mal placé n'aurait pas accès aux bons outils et pourrait hériter de droits inadaptés. On effectue donc un couper-coller du compte depuis le conteneur générique vers l'OU correspondant au service de l'utilisateur.

Name	Type
CDG	Organizational Unit
CEL	Organizational Unit
CHOD	Organizational Unit
Comptes_desactives	Organizational Unit
Comptes_Industriels	Organizational Unit
Contacts	Organizational Unit
DESIGN	Organizational Unit
DF_RECS	Organizational Unit
DIRECTION	Organizational Unit
EFEL	Organizational Unit
GA_Synergy	Organizational Unit
HR	Organizational Unit
INDUS	Organizational Unit
Infra	Organizational Unit
IT	Organizational Unit
LPF	Organizational Unit
QSE	Organizational Unit
SATC	Organizational Unit
Users_Admin	Organizational Unit
WorkspaceOne	Organizational Unit





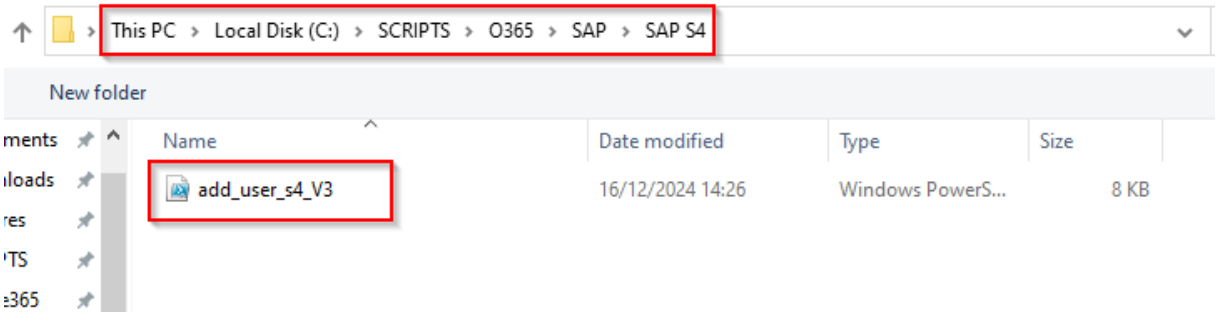
Étape 4 –

Vérification et correction de la configuration : On contrôle les propriétés du compte dans l'AD : nom complet, adresse mail, service, numéro de téléphone, groupes d'appartenance. Cette étape garantit la cohérence des informations dans l'annuaire, notamment pour le carnet d'adresses Outlook et les accès aux

ressources partagées. Des corrections sont apportées si nécessaire avant toute notification à l'utilisateur.

Étape 5 –

Attribution de l'accès SAP (si nécessaire) : Si l'utilisateur a besoin d'utiliser le logiciel SAP, il faut ajouter l'attribut 10 dans les propriétés de son compte AD. Certains collaborateurs (principalement les services logistique, production et achats) ont besoin d'accéder à SAP, l'ERP du Groupe Atlantic. L'ajout de cet attribut spécifique dans les propriétés AD est lu par le système SAP lors de l'authentification pour autoriser la connexion. Cette étape est réalisée uniquement sur demande explicite du responsable du service concerné.



Étape 6 –

Exécution du script de finalisation : Un script PowerShell est exécuté en renseignant le login de l'utilisateur. Ce script réalise automatiquement les dernières configurations nécessaires : initialisation de la boîte mail dans Exchange, application des droits de base, synchronisation avec Azure AD (Entra ID) pour les services cloud Microsoft 365. L'automatisation via script évite les erreurs de manipulation manuelle et garantit un compte conforme à la politique du groupe.

À partir de là, l'utilisateur est entièrement configuré et peut se connecter à l'environnement Windows et Microsoft Office 365. Les identifiants (login et mot de passe provisoire) lui sont transmis via son responsable, accompagnés d'une note l'invitant à changer son mot de passe dès la première connexion, conformément à la politique de sécurité du Groupe Atlantic.

MISSION 2 : Intégration d’un macOS dans l’AD

Mise en situation

Le service IOT (Internet of Things) à régulièrement besoin de travailler sur macOS pour des projets spécifiques liés à l'écosystème Apple. Cependant, macOS n'est pas le standard dans le Groupe Atlantic : l'infrastructure est basée sur Windows et Active Directory. L'enjeu de cette mission est donc d'intégrer ces machines non-standard dans le domaine tout en garantissant leur conformité de sécurité (antivirus, gestion de parc, VPN). Une procédure stricte a été définie par la DSI du groupe, et c'est cette procédure que je dois appliquer à chaque nouvel appareil.

Ma mission

Étape 1 –

Initialisation et sécurisation du compte administrateur local : Lors du premier démarrage du MacOS neuf, on crée un compte administrateur local (identifiant : admin) avec un mot de passe de 20 caractères généré aléatoirement et stocké dans KeePass, le gestionnaire de mots de passe sécurisé du service informatique. Ce compte local sert de base de travail lors de la configuration initiale et permet d'intervenir en cas de problème avec les comptes du domaine. L'utilisation d'un mot de passe fort et unique enregistré dans KeePass est une bonne pratique de sécurité essentielle : elle évite l'usage de mots de passe triviaux ou réutilisés.

Étape 2 –

Nommage de la machine : Le nom du MacBook doit être GA+SerialNumber et pour que ce nom soit « complètement » effectif sur le Mac, il faut passer ces commandes dans un terminal :

- sudo scutil --set ComputerName "GA+SerialNumber"
- sudo scutil --set LocalHostName "GA+SerialNumber"
- sudo scutil --set HostName "GA+SerialNumber"

Exécuter les commandes suivantes en ligne de commande :

- sudo -i

Étape 3 – Jonction au domaine Active Directory : La commande dsconfigad est l'outil natif macOS pour rejoindre un domaine Active Directory. Elle est lancée avec les paramètres du domaine Groupe Atlantic, en précisant l'OU de

destination, les options de mobilité (mobile enable) et les groupes AD autorisés à administrer la machine. L'utilisation d'un compte privilégié (a-AdminRISAccount) est nécessaire pour effectuer cette opération. Une fois la commande exécutée avec succès, le Mac est membre du domaine et les comptes AD peuvent s'y authentifier. Commande : dsconfigad -a **GA+SerialNumber** -u **a-AdminRISAccount** -ou "OU=Unclassified_Computers,DC=groupe-atlantic,DC=com" -domain groupe-atlantic.com -mobile enable -mobileconfirm enable -localhome enable -useuncpath enable -groups "Domain Admins,Enterprise Admins,UG_RIS_FRLRM" -alldomains enable

/!\ AdminRISAccount = compte a-

Étape 4 –

Déplacement dans l'AD et mise à jour de la cartographie : Comme pour les postes Windows, le Mac est déplacé depuis l'OU par défaut vers l'OU adaptée dans l'AD. Il est également renommé selon la convention GA+SerialNumber. La cartographie du parc informatique est mise à jour pour que le service IT garde une vision précise de l'inventaire (localisation, utilisateur, système d'exploitation). Cette traçabilité est indispensable en cas d'audit ou d'incident de sécurité.

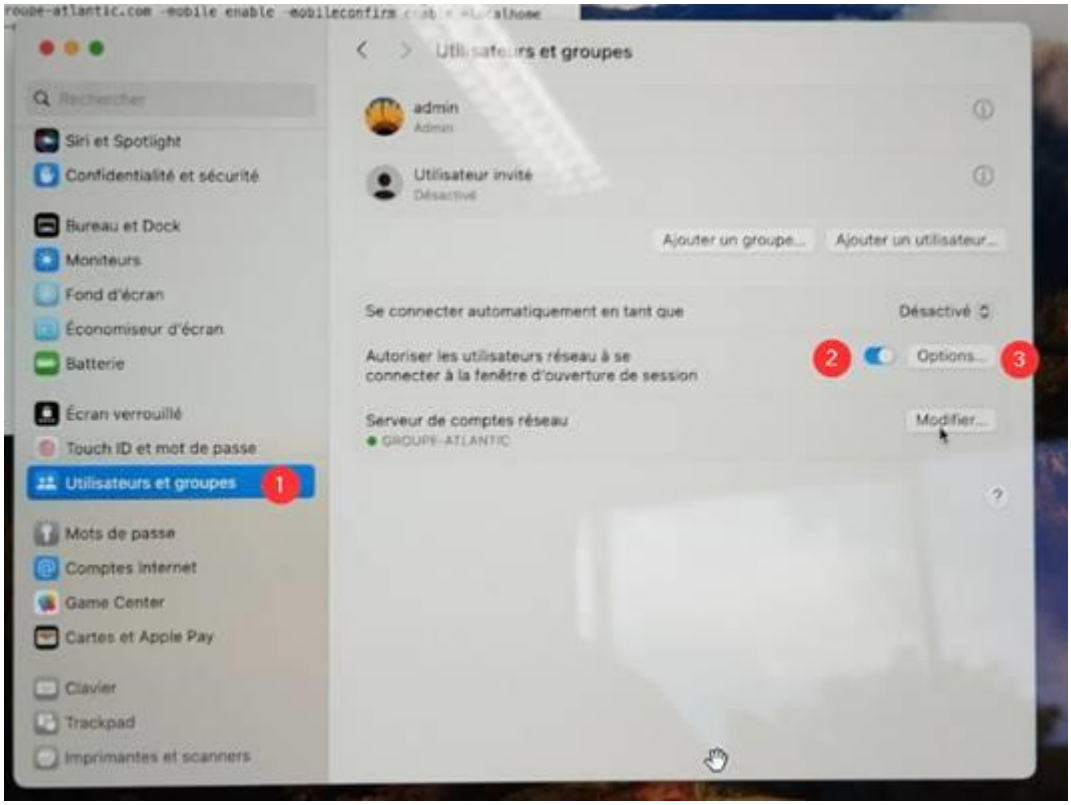
Pour autoriser l'ouverture de session sur le MacOS par des comptes de l'AD, il faut intégrer les paramètres suivants :

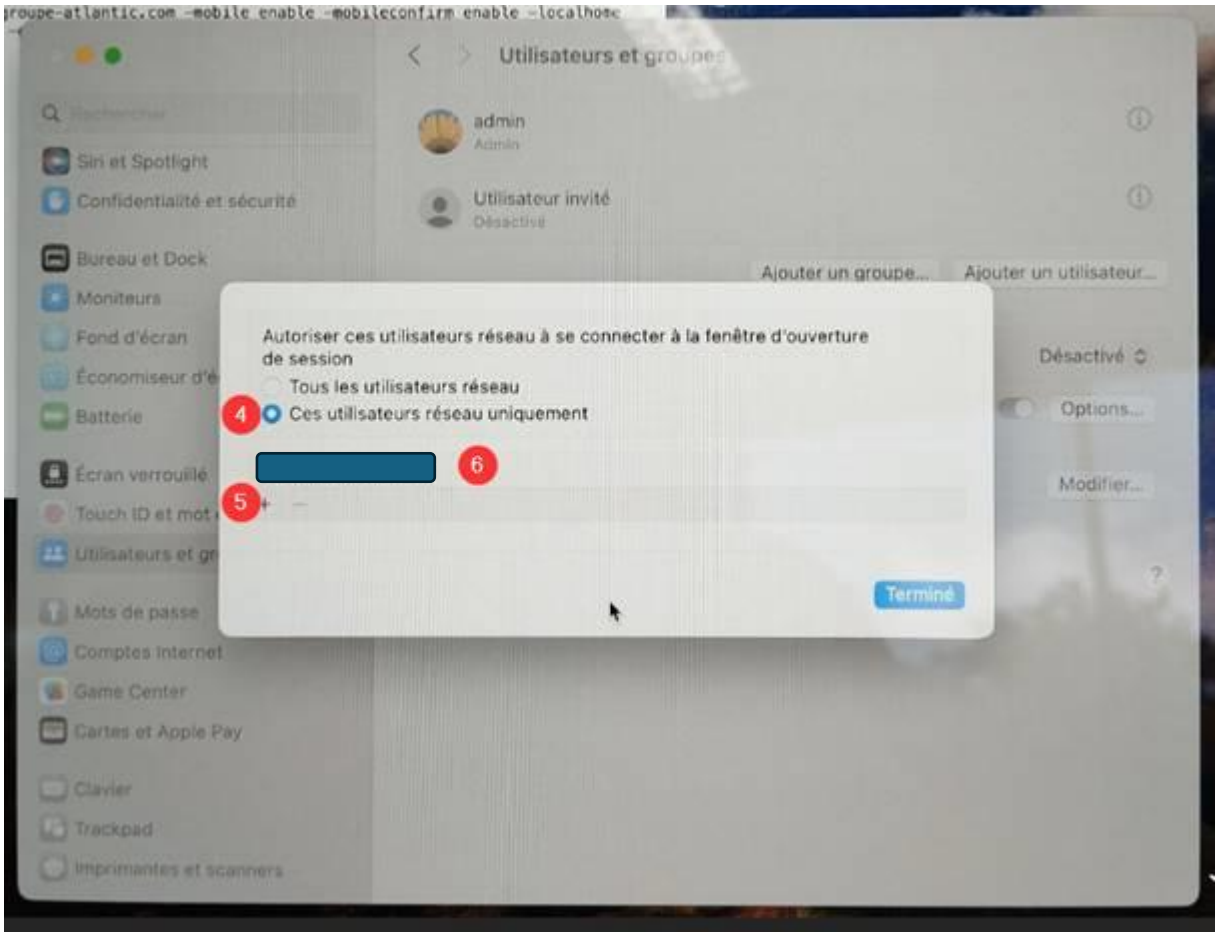
- Dans Réglages Systèmes > Utilisateurs et groupes, Options > les éléments suivants doivent être cochés :

o Autoriser les utilisateurs réseau à se connecter à la fenêtre d'ouverture de session

▪ Sélectionner Ces utilisateurs réseau uniquement

▪ Sélectionner **l'utilisateur du MAC** dans la liste


Utilisateurs et groupes
admin
Admin
Utilisateur invité
Désactivé
Ajouter un groupe...
Ajouter un utilisateur...
Se connecter automatiquement en tant que
Désactivé
Autoriser les utilisateurs réseau à se connecter à la fenêtre d'ouverture de session
Options...
Serveur de comptes réseau
Modifier...
Siri et Spotlight
Confidentialité et sécurité
Bureau et Dock
Moniteurs
Fond d'écran
Économiseur d'écran
Batterie
Écran verrouillé
Touch ID et mot de passe
Utilisateurs et groupes
Mots de passe
Comptes Internet
Game Center
Cartes et Apple Pay
Clavier
Trackpad
Imprimantes et scanners
1
2
3

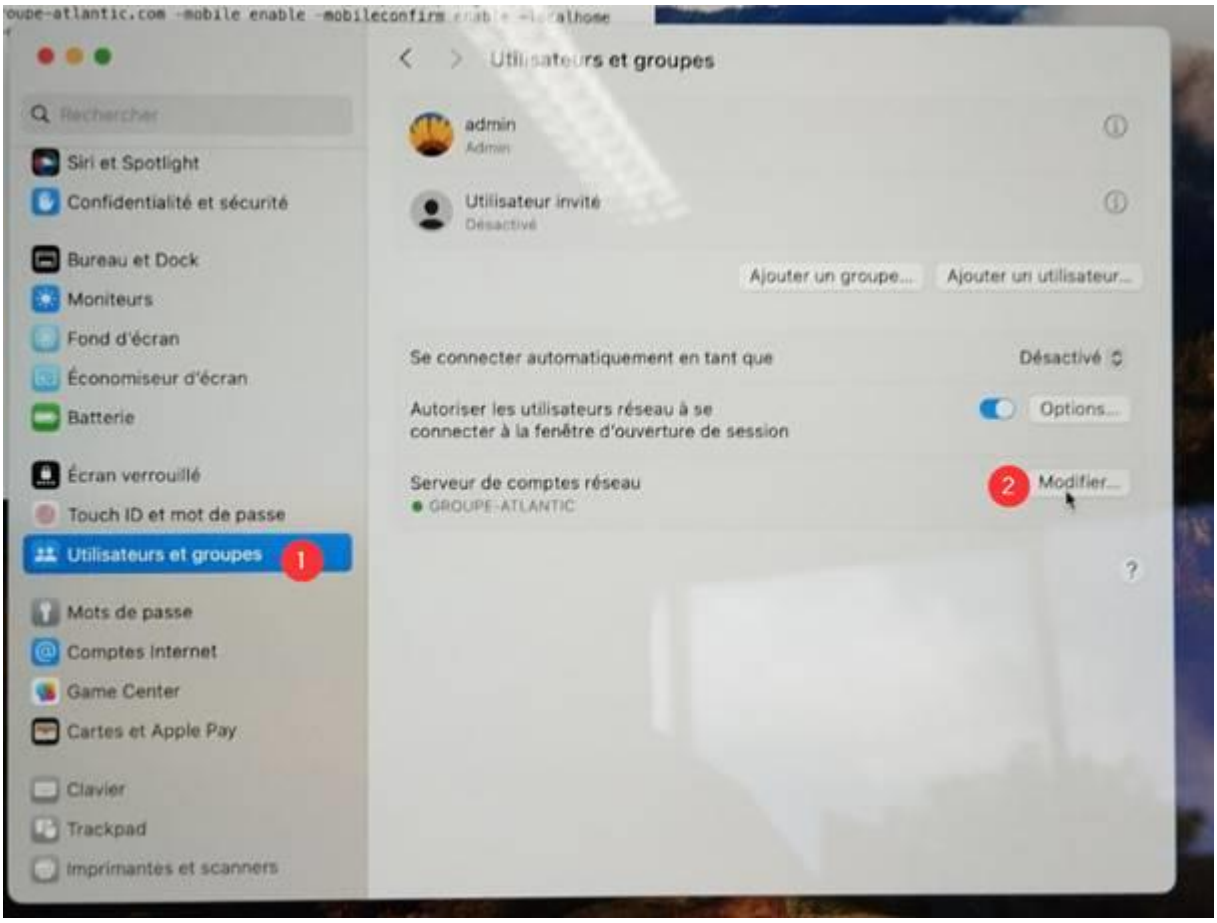


Étape 5 –

Attribution des droits administrateurs à l'utilisateur : L'utilisateur du service IOT a besoin de droits administrateurs locaux sur son Mac pour installer certains outils de développement. Ces droits sont accordés via les paramètres du système macOS, en ajoutant son compte AD dans la liste des administrateurs. Cette étape est contrôlée et limitée aux cas justifiés, car accorder des droits admin à tout utilisateur représenterait un risque de sécurité important.

Étape 6 –

Configuration avancée de l'intégration AD : Dans l'Utilitaire d'annuaire macOS, on configure les paramètres de liaison avec l'Active Directory : création d'un compte mobile à l'ouverture de session (pour s'authentifier même hors réseau), définition du groupe UG_RIS_FRLRM comme groupe d'administration, et autorisation de s'authentifier depuis n'importe quel domaine de la forêt. Ces réglages garantissent que la machine fonctionne correctement tant en mode connecté qu'en mobilité. On accède à ces paramètres via

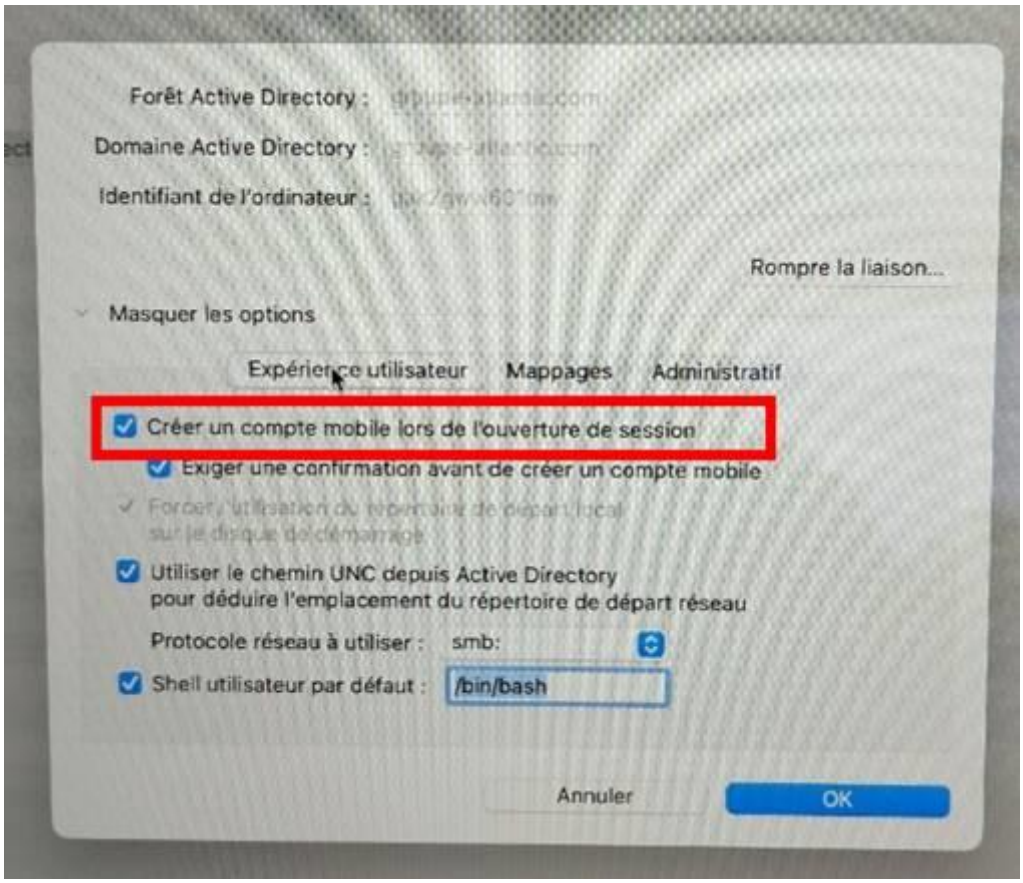


o Sélectionner Ouvrir Utilitaire d'annuaire

o Déverrouiller et sélectionner Active Directory

o Dans l'onglet Expérience utilisateur :

▪ Sélectionner Créer un compte mobile lors de l'ouverture de session

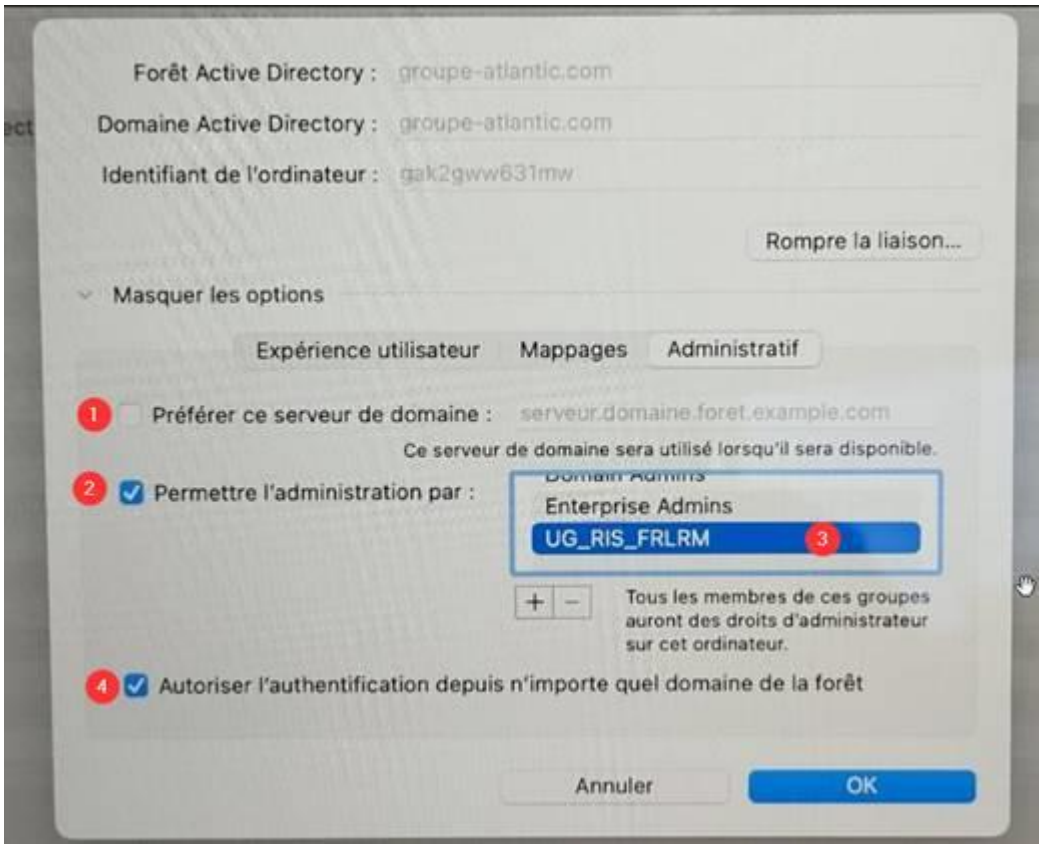


o Dans l'onglet Administratif :

▪ Ne pas sélectionner Préférer ce serveur de domaine

▪ Permettre l'administration par : le nom du groupe UG de l'AD contenant les comptes d'administration de l'équipes RIS (**UG_RIS_FRLRM**)

▪ Sélectionner Autoriser l'authentification depuis n'importe quel domaine de la forêt

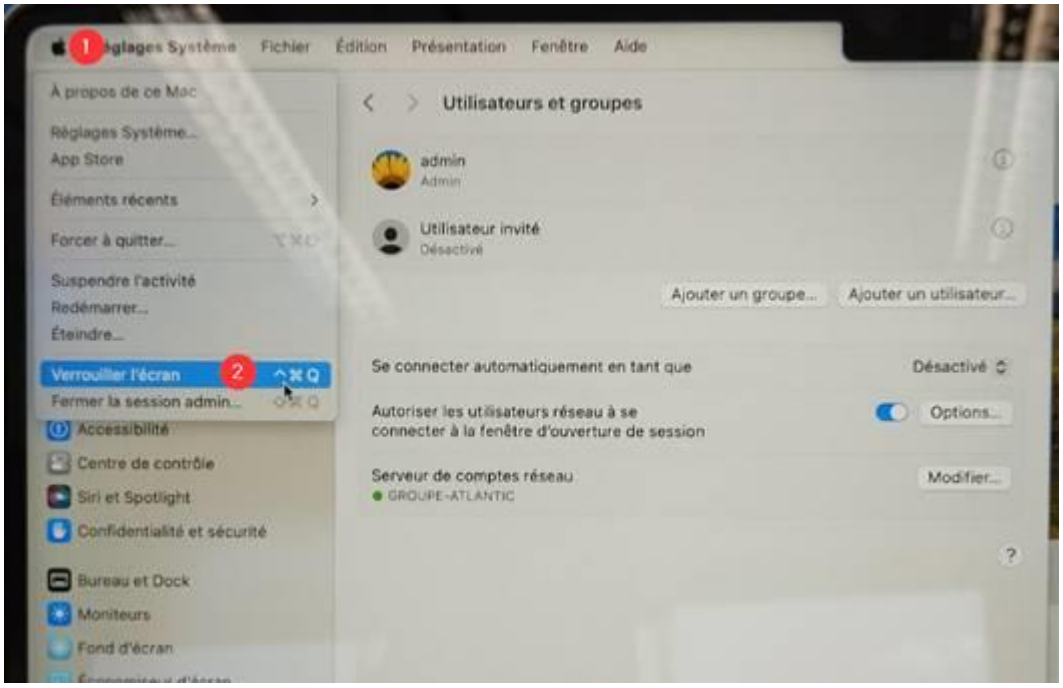

Forêt Active Directory : groupe-atlantic.com
Domaine Active Directory : groupe-atlantic.com
Identifiant de l'ordinateur : gak2gww631mw
Rompre la liaison...
Masquer les options
Expérience utilisateur
Mappages
Administratif
1
Préférer ce serveur de domaine :
serveur.domaine.foret.example.com
Ce serveur de domaine sera utilisé lorsqu'il sera disponible.
2
Permettre l'administration par :
Enterprise Admins
UG_RIS_FRLRM
3
Tous les membres de ces groupes auront des droits d'administrateur sur cet ordinateur.
4
Autoriser l'authentification depuis n'importe quel domaine de la forêt
Annuler
OK

Étape 7 –

Première connexion avec le compte AD : On teste la connexion au Mac avec le compte Active Directory de l'utilisateur pour vérifier que l'intégration au domaine fonctionne correctement. Depuis le compte admin local, on verrouille le poste puis on s'authentifie avec le login et mot de passe AD de l'utilisateur. Cette étape valide que le Mac est bien joint au domaine et que l'utilisateur peut ouvrir une session.

Demander le mdp AD de l'utilisateur

Depuis le compte admin : verrouiller le poste



Puis sur l'écran de login : sélectionner Autre

Enfin, saisir le login et le mdp du user

Étape 8 –

Connexion au réseau Wi-Fi dédié : Les Mac et appareils Linux ne peuvent pas se connecter au réseau Wi-Fi standard de l'entreprise. Un SSID spécifique (GAOFFICEOSX) leur est réservé, utilisant un système PPSK (Private Pre-Shared Key) : chaque appareil dispose d'une clé unique générée dans le contrôleur Wi-Fi. Cette approche isole les appareils non-standards du réseau principal, ce qui réduit la surface d'attaque en cas de compromission. La procédure de génération de cette clé est détaillée en annexe.

Donner un accès au réseau GAOFFICEOSX à l'utilisateur en suivant le modop suivant :

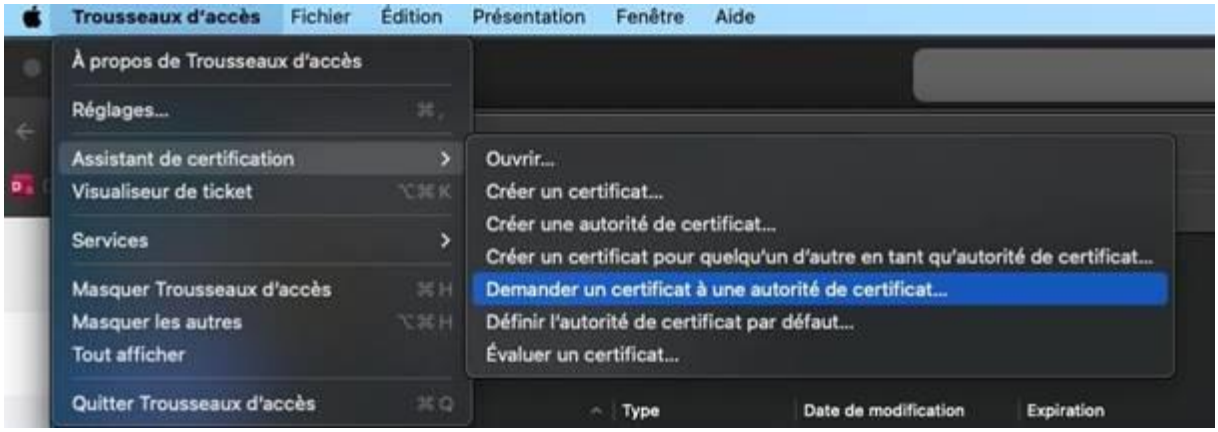
SSID---GAOFFICEOSX (voir Annexe p.46)

Connecter le réseau sur le mac en saisissant le mdp généré.

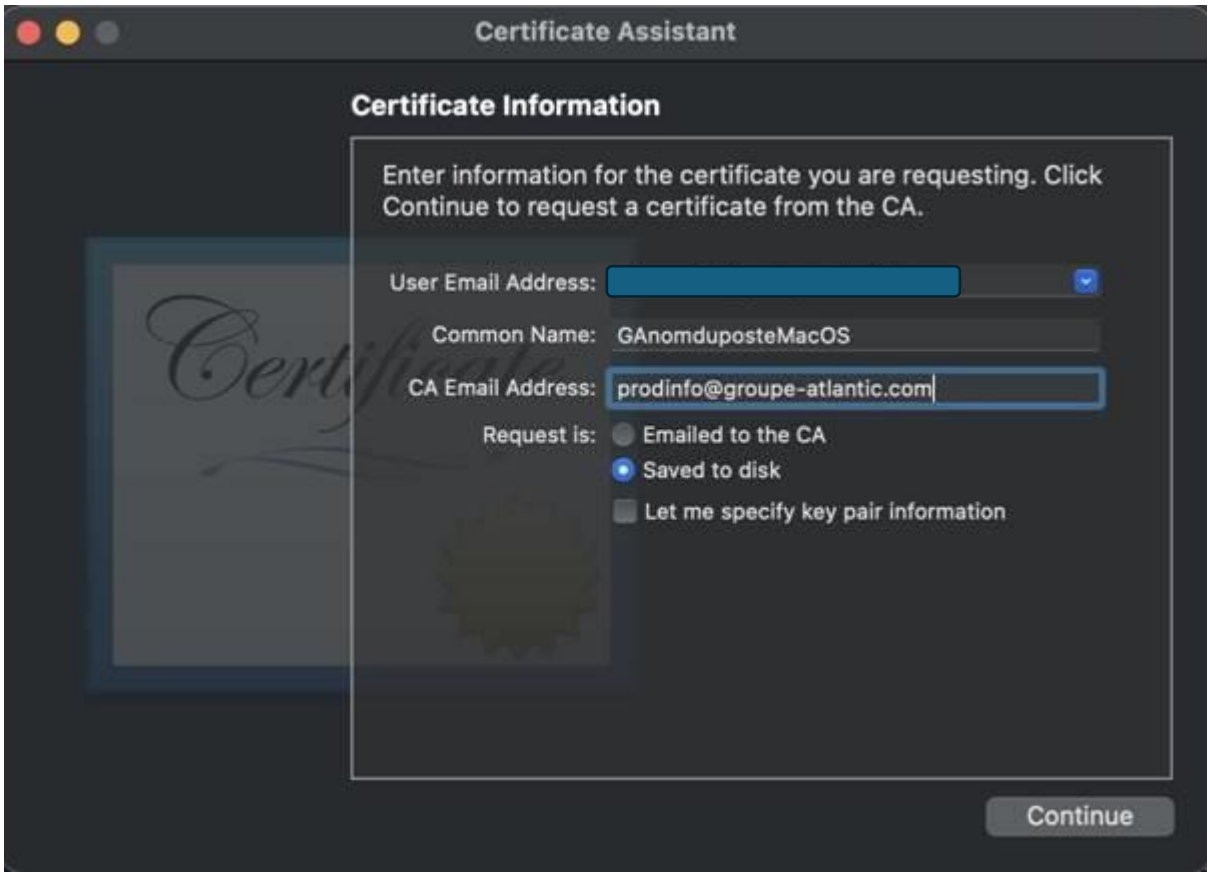
Étape 9 –

Création et installation du certificat pour le MacOS (depuis le compte du user)

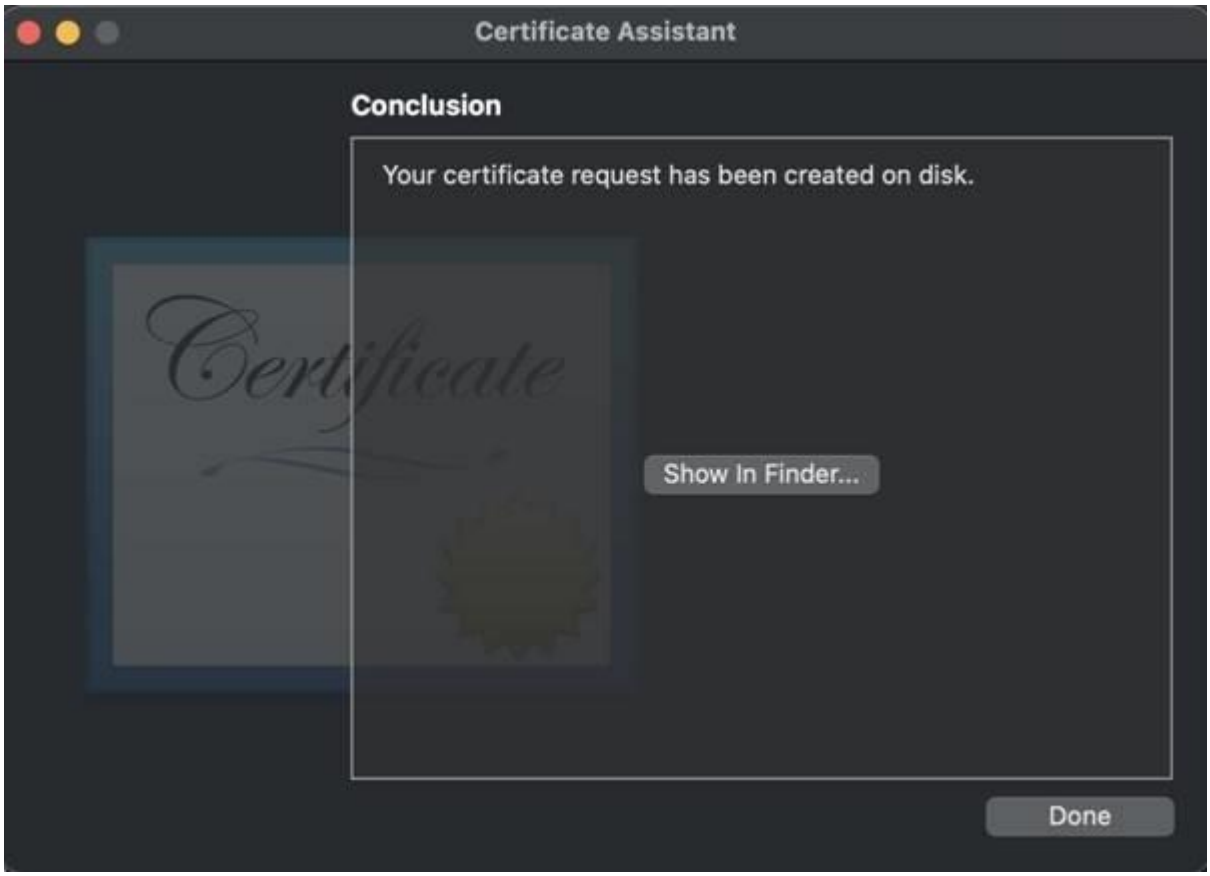
Générer un certificat local pour le signer. Lancer l'application « Trousseaux d'accès »



Common Name = nom du MacOS



CA email address = prodinfo@groupe-atlantic.com

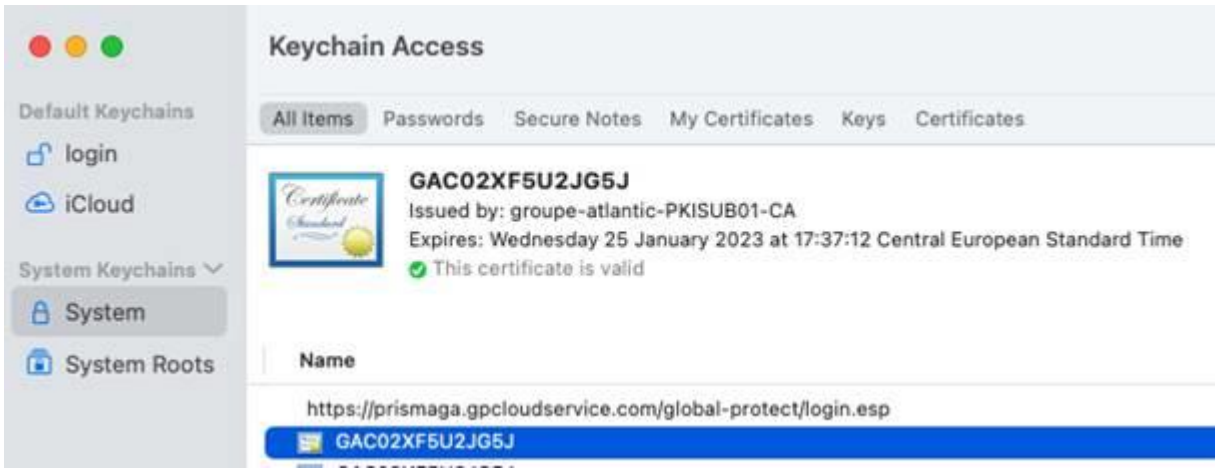


Enregistrer le certificat sous ce modèle de nom

Générer le certificat signé en suivant la procédure :

APPLE-MAC-Management (Voir annexe p.50)

Importer le fichier dans le mac, double cliquer dessus et autoriser avec le compte admin.



Il faut ensuite ajouter les certificats racines du Domaine Groupe Atlantic :

- Se connecter à l'url http://pkiweb01.groupe-atlantic.com/aia/

- Télécharger et installer les certificats dans le magasin.

o Dans l'app Trousseaux d'Accès sur votre Mac, sélectionner le trousseau Système.

o Faire glisser le fichier de certificat sur l'app Trousseaux d'accès.

o S'il est demandé de fournir un nom et un mot de passe, taper le nom et le mot de passe d'un utilisateur administrateur local de l'ordinateur.

- Sur le certificat de la ROOT CA, un message d'alerte disant que ce n'est pas approuvé.

- Modifier les paramètres pour le rendre fiable.

- Refermer l'App Trousseaux d'Accès

Étape 10 –

Installation de KACE (gestion de parc) : KACE est l'outil de gestion de parc informatique (MDM) du Groupe Atlantic. Son installation est obligatoire sur tous les appareils, y compris les Mac : il permet à l'équipe IT de déployer des mises à jour, de

faire des inventaires matériels et logiciels, et d'intervenir à distance si nécessaire. Sans KACE, le Mac est invisible pour l'équipe informatique et considéré comme non-conforme.

Récupérer la dernière version MAC de KACE ici : \\nasga\sources$\Software\Quest\Kace

Installer KACE en faisant suivant (les paramètres par défaut sont OK)

Étape 11 –

Installation de Cortex XDR (antivirus) : Cortex XDR de Palo Alto Networks est la solution antivirus et EDR (Endpoint Detection and Response) déployée sur l'ensemble du parc Atlantic. Son installation est obligatoire sur les Mac non-standard : il protège contre les malwares, surveille les comportements suspects et remonte les alertes vers la DSI. C'est l'une des conditions sine qua non à l'utilisation d'un Mac sur le réseau de l'entreprise.

Récupérer la dernière version MAC de cortex ici : \\nasga\sources$\Software\Antivirus

Installer Cortex en faisant suivant (les paramètres par défaut sont OK)

Activer toutes les autorisations demandées dans les différents écrans suivants

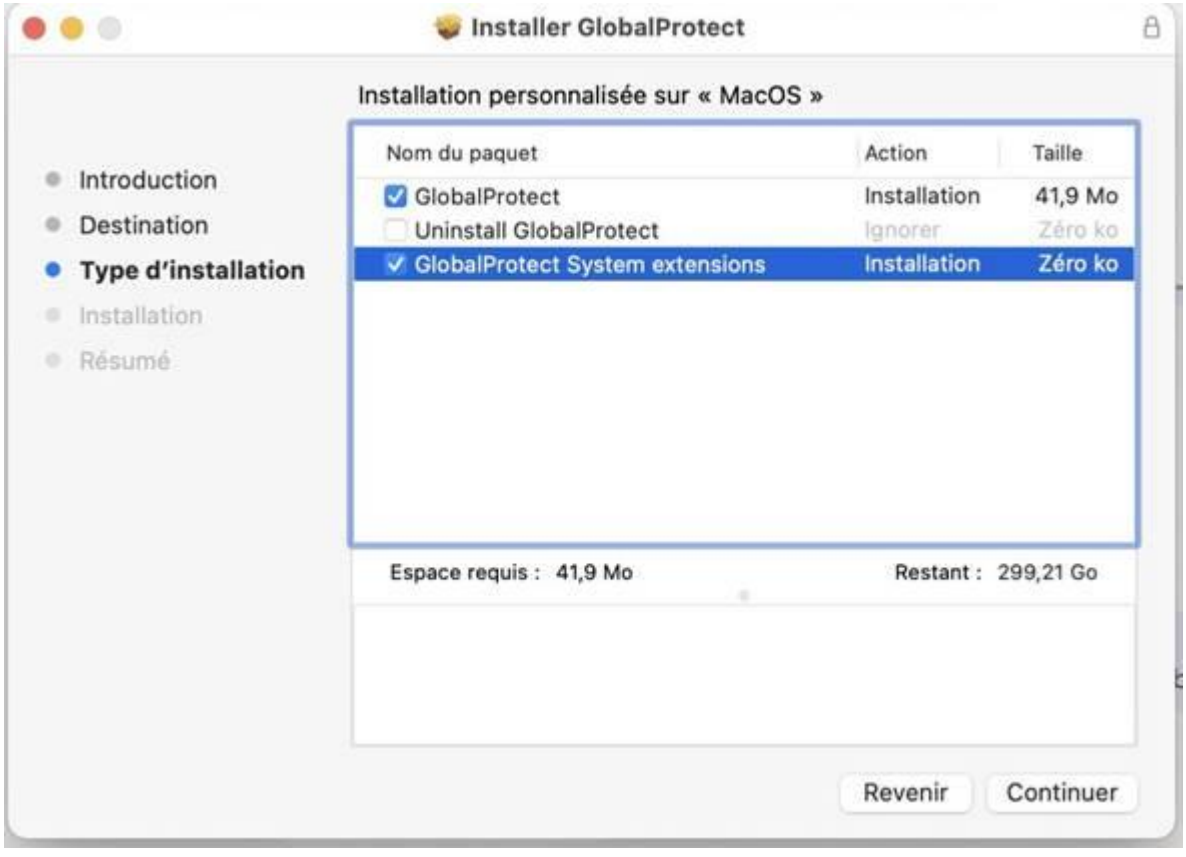
Étape 12 –

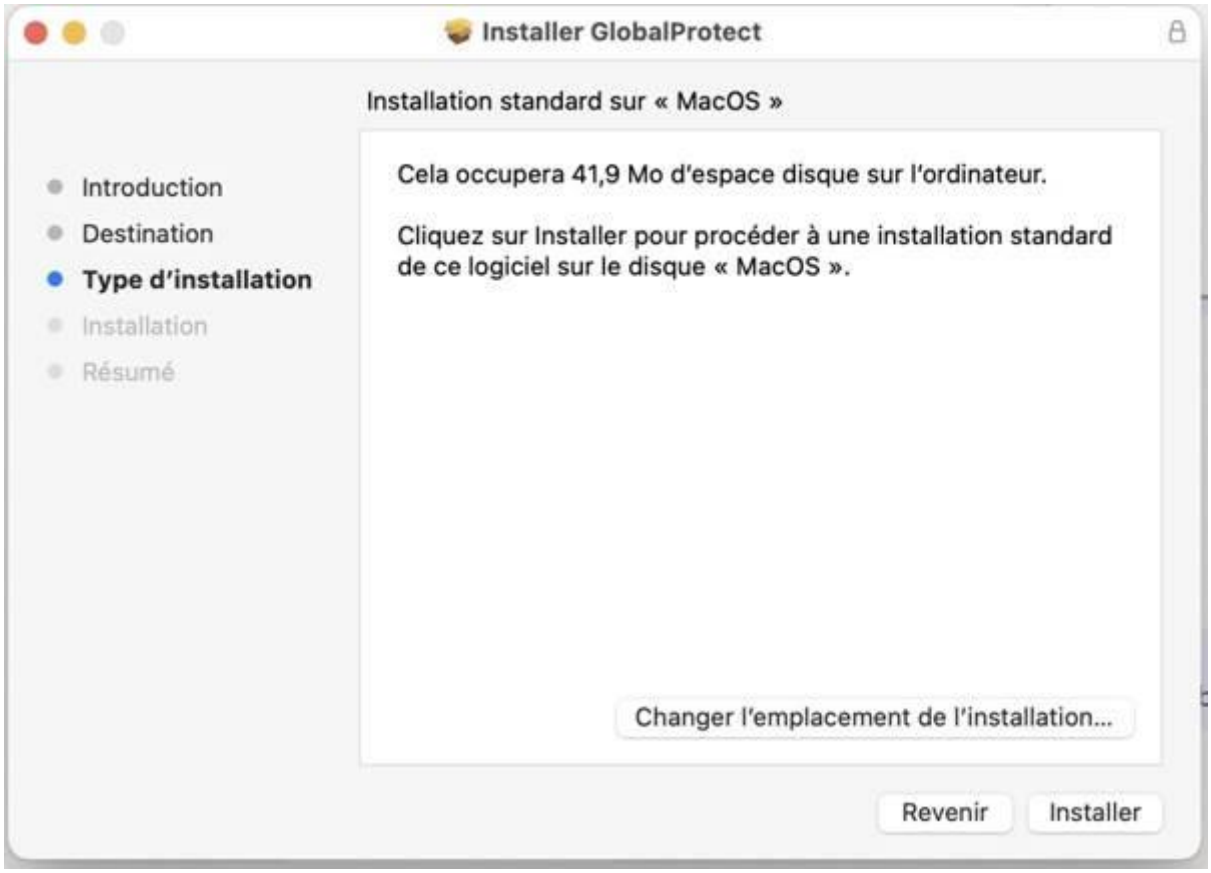
Installation et configuration du VPN GlobalProtect : GlobalProtect est la solution VPN de Palo Alto utilisée par le Groupe Atlantic. Elle permet aux utilisateurs de se connecter au réseau interne depuis l'extérieur (télétravail, déplacement). La configuration nécessite l'installation de l'agent, l'ajout des extensions système GlobalProtect, l'autorisation d'accès aux certificats du trousseau macOS et la saisie de l'adresse du portail (prismaga.gpcloudservice.com). Une première connexion depuis un réseau extérieur (box personnelle ou partage 4G) est indispensable pour récupérer les paramètres de détection automatique du réseau interne.

Récupérer la dernière version MAC ici : \\nasga\sources$\Software\PaloAlto\Global Protect

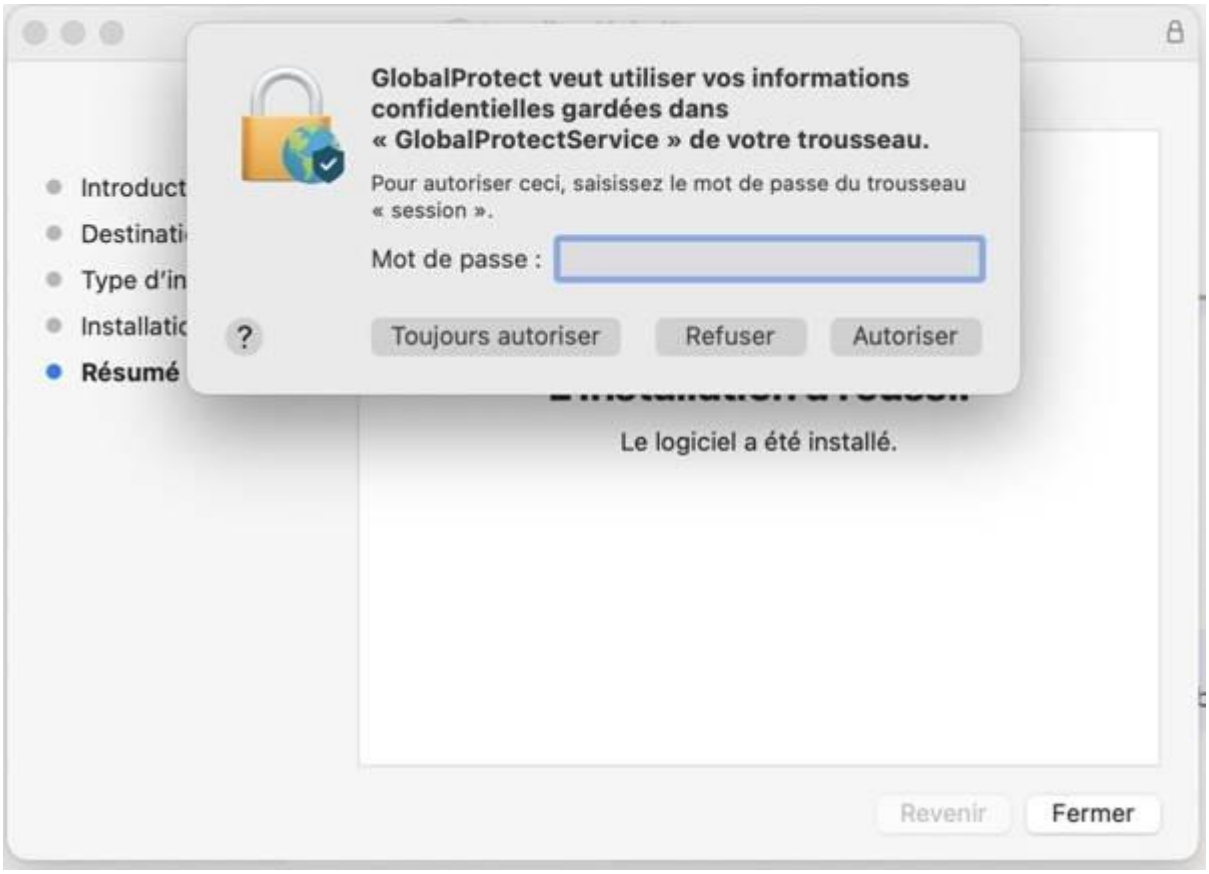
Lancer l'installation

Ajouter GlobalProtect System extensions

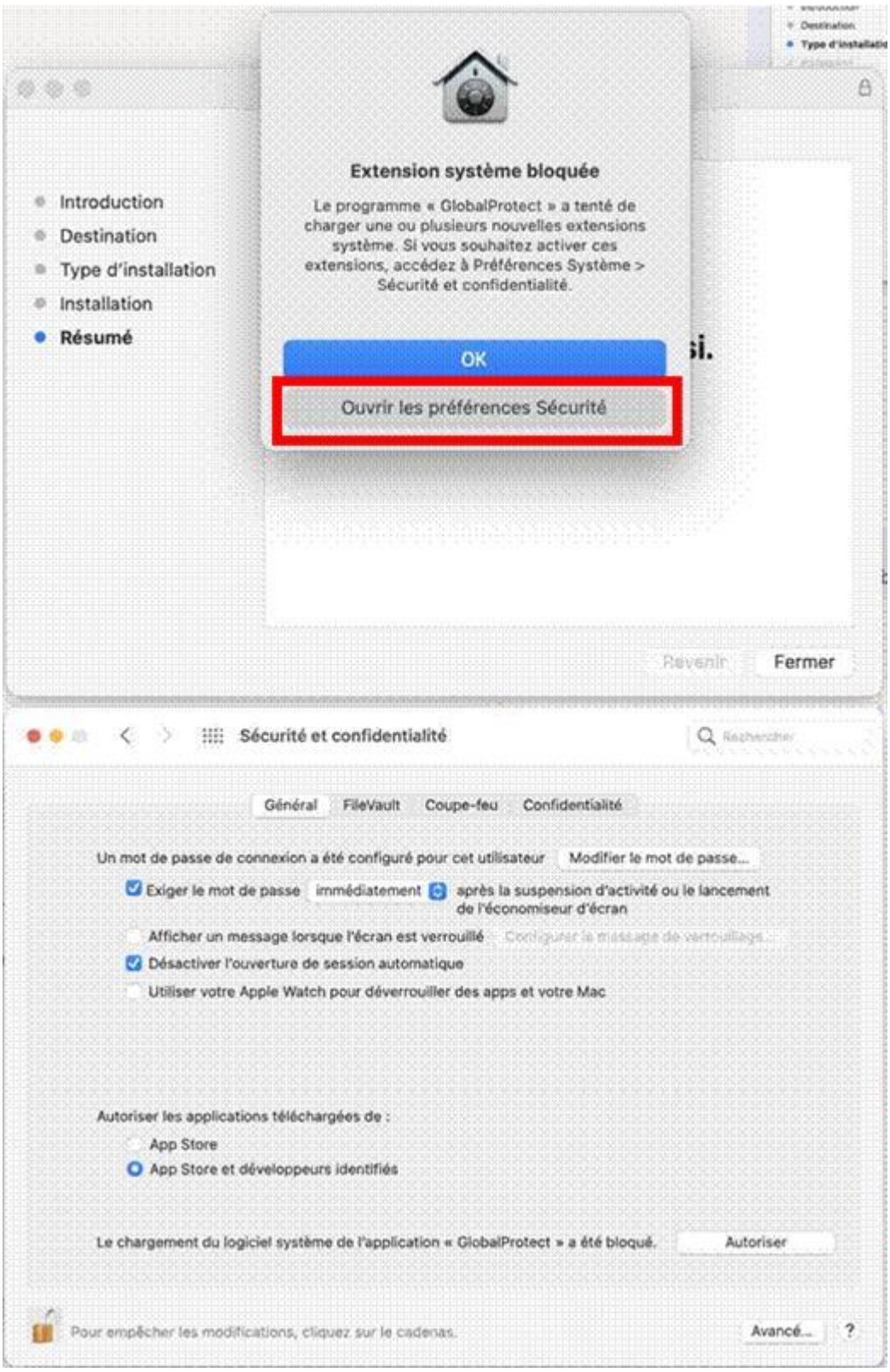




Saisir le mot de passe du compte local MacOS et cliquer sur « toujours autoriser » pour que GP accède aux certificats.



Autoriser les extensions GlobalProtect dans les préférences de sécurité


Introduction
Destination
Type d'installation
Installation
Résumé
Extension système bloquée
Le programme « GlobalProtect » a tenté de charger une ou plusieurs nouvelles extensions système. Si vous souhaitez activer ces extensions, accédez à Préférences Système > Sécurité et confidentialité.
OK
Ouvrir les préférences Sécurité
Revenir
Fermer
Sécurité et confidentialité
Général
FileVault
Coupe-feu
Confidentialité
Un mot de passe de connexion a été configuré pour cet utilisateur
Modifier le mot de passe...
Exiger le mot de passe
immédiatement
après la suspension d'activité ou le lancement de l'économiseur d'écran
Afficher un message lorsque l'écran est verrouillé
Désactiver l'ouverture de session automatique
Utiliser votre Apple Watch pour déverrouiller des apps et votre Mac
Autoriser les applications téléchargées de :
App Store
App Store et développeurs identifiés
Le chargement du logiciel système de l'application « GlobalProtect » a été bloqué.
Autoriser
Pour empêcher les modifications, cliquez sur le cadenas.
Avancé...
?

Étape 13 –

Activation et test de GlobalProtect : Après installation, on active le VPN en renseignant l'adresse du portail et en s'authentifiant avec le compte AD/O365 de l'utilisateur. Le certificat préalablement signé (CSR) doit également être ajouté au trousseau pour permettre l'authentification client. La détection du réseau est ensuite automatique : quand l'utilisateur est sur le réseau interne de l'entreprise, le VPN ne se connecte pas ; depuis l'extérieur, il se connecte automatiquement, assurant une sécurité transparente pour l'utilisateur.

Ajouter l'adresse du portail **prismaga.gpcloudservice.com**

S'authentifier avec le compte AD / O365 et « toujours autoriser » l'accès au trousseau.

Bien évidemment, le GAnomduposteMacOS.csr signé a été préalablement ajouté par vos soins à votre trousseau.

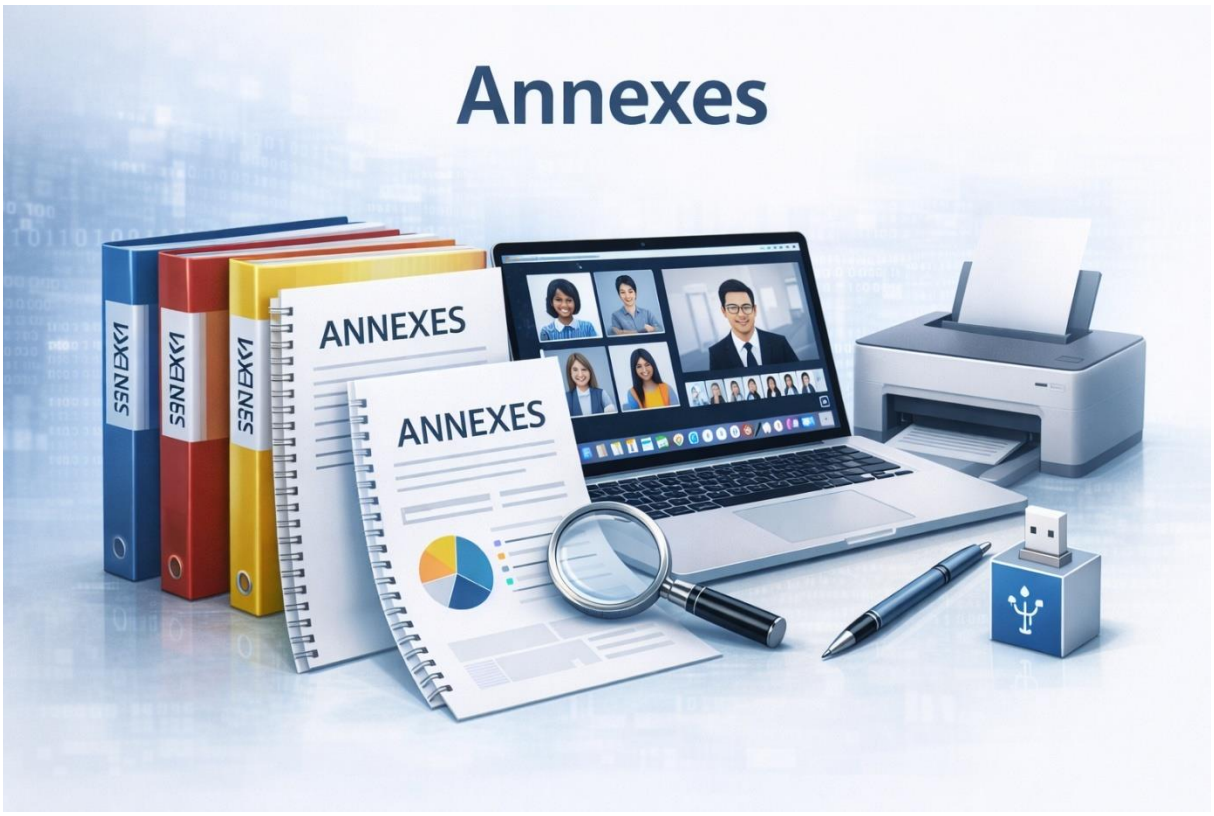
Une première connexion sur un réseau externe (box perso ; partage de co' 4G) est nécessaire pour récupérer les paramètres GP. Ensuite, la détection du réseau est automatique.

Conclusion

Au cours de mon alternance au sein du service informatique d'Atlantic Industrie, j'ai participé à plusieurs missions concrètes d'administration système et de gestion des comptes utilisateurs : création de comptes Active Directory, attribution de licences Microsoft 365 et intégration de postes macOS dans le domaine.

Ces missions m'ont permis de développer des compétences techniques solides, de mieux comprendre le fonctionnement d'une infrastructure d'entreprise et de mesurer l'importance des procédures et de la sécurité dans un environnement industriel.

Cette expérience en alternance a renforcé mon intérêt pour les systèmes, les réseaux et la cybersécurité. Elle m'a également appris à travailler en équipe, à respecter des procédures strictes et à m'adapter aux contraintes d'un environnement professionnel exigeant. À l'issue de ce BTS SIO option SISR, je souhaite poursuivre dans ce domaine, que ce soit par une licence professionnelle en sécurité des systèmes d'information ou en intégrant directement le monde du travail en tant qu'administrateur systèmes et réseaux.


Annexes
ANNEXES
ANNEXES

SSID - GAOFFICEOSX

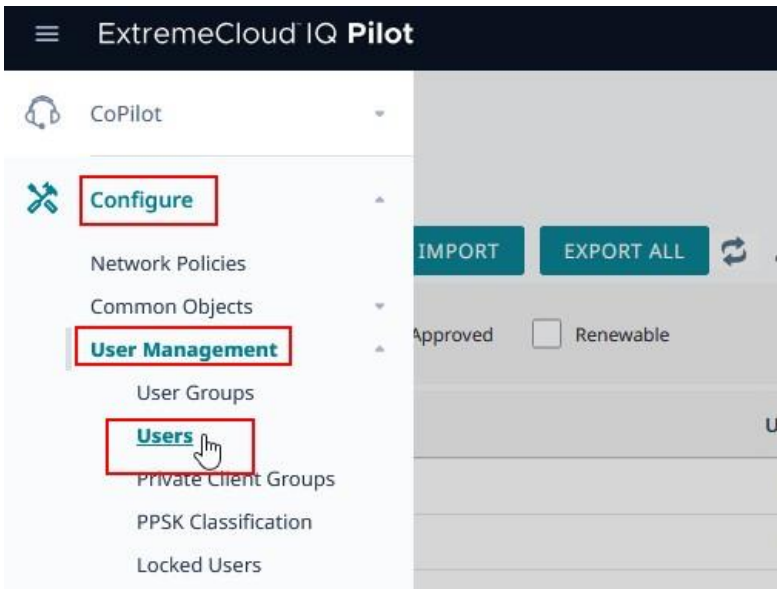
This SSID is **only** available for specific devices with an operating system such as MAC OS or Linux.

This SSID uses the PPSK as security key. The security key can be communicated to the user. It is unique and dedicated for the devices.

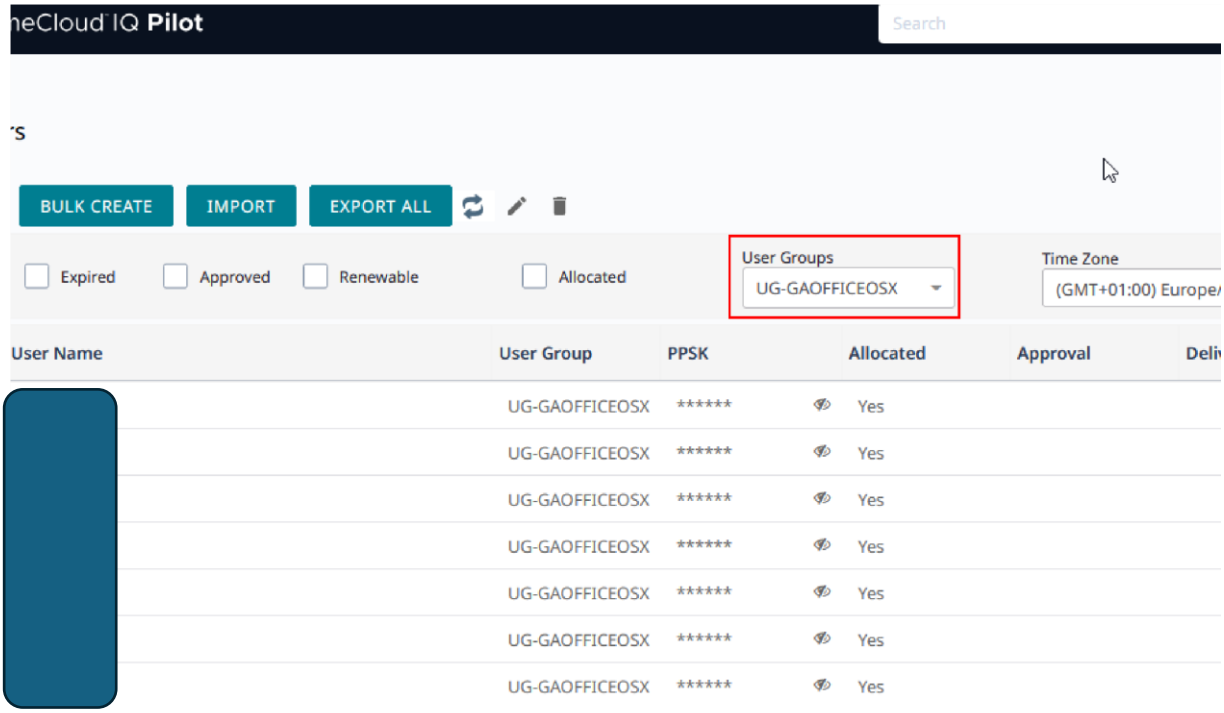
Important : This key can only be used on one device at a time. And it must only be used for corporate devices.

How to create a new security Key

As mention before, there will are one key per device for this SSID. Go the menu **Configure** > **User Management** > **Users** :



In the users screen, you can select the following user groups:
UG_GAOFFICESOSX



You will be able to see all users already created.

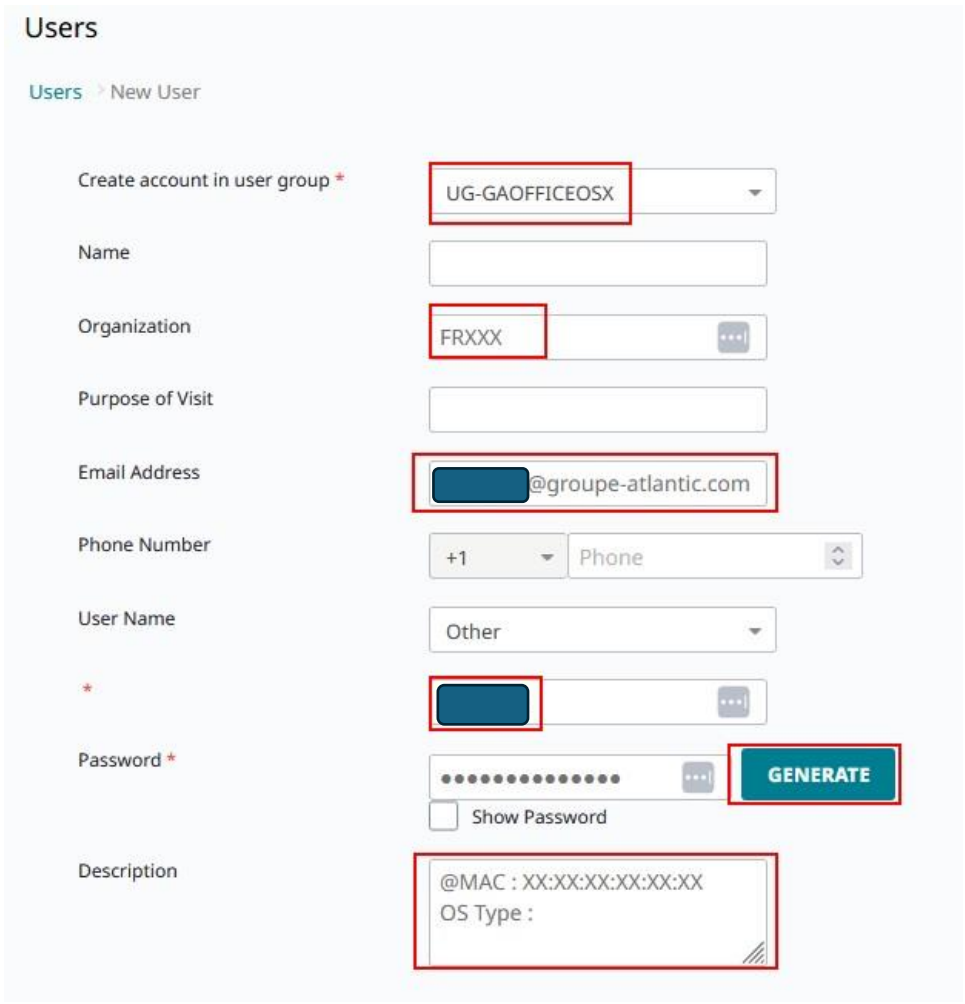
If you want to add a new one, click on the button **+**:

Complete these informations :

SSID - GAOFFICEOSX

- Create account in user group : UG_GAOFFICESOSX
- Organization : Site Pentagrams Email address select
- other for username and enter the windows login
- Generate password

Description : Indicate the mac address and the operating system



Once you have completed all required information, you can click on the buton “**save**”

You will be able to connect to the SSID with the new PPSK.

APPLE MAC _ Linux Management

INTRODUCTION

Mac or Linux computers are not the standard within our group and should only be used for exceptional purposes **NO SUPPORT WILL BE PROVIDED ON THESE DEVICES**

Groupe-Atlantic resources access

The preferred method to access the group resources is to use a citrix connection.

Global Protect Access (NOT RECOMENDED)

The global protect access is not recommended but here is the procedure to get a certificate.

Prerequisites

Cortex and **KACE** are **MANDATORY** on these devices.

Get the CSR (Certificate Signing Request)

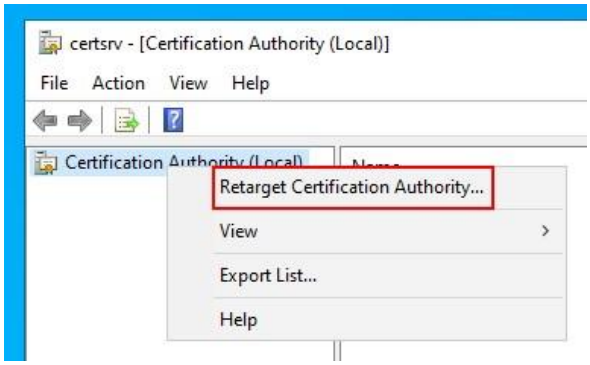
Generate a csr file on the computer and save it.

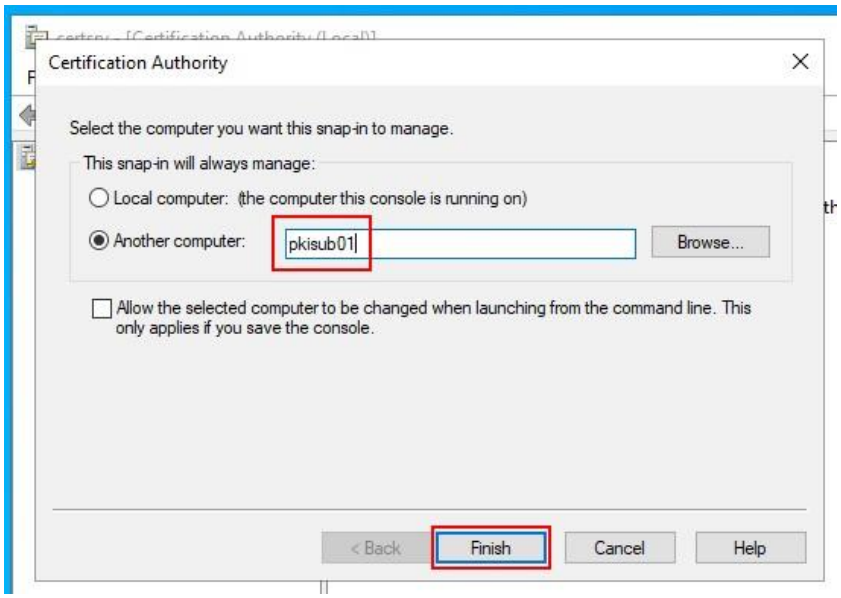
Update the certificate template

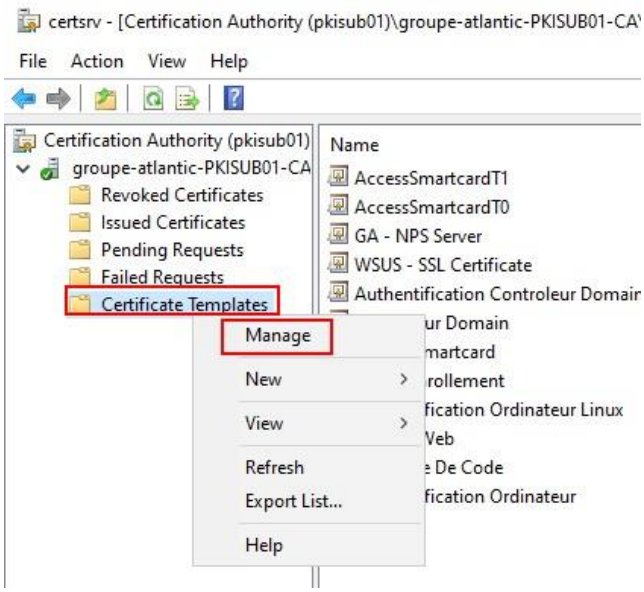
With an account that has the required permission, connect to a T2 Citrix administration server (with a- account).

You may need to retarget the Certification Authority if you encounter this message:

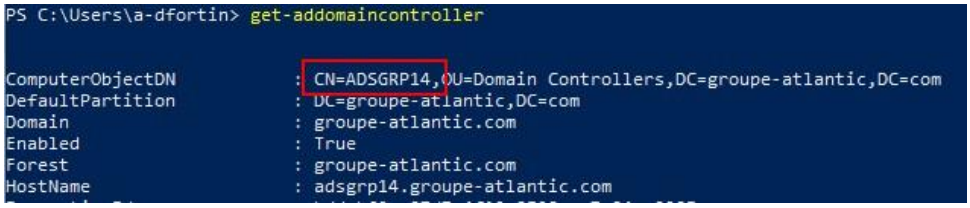
Click OK and Retarget Certification Authority.



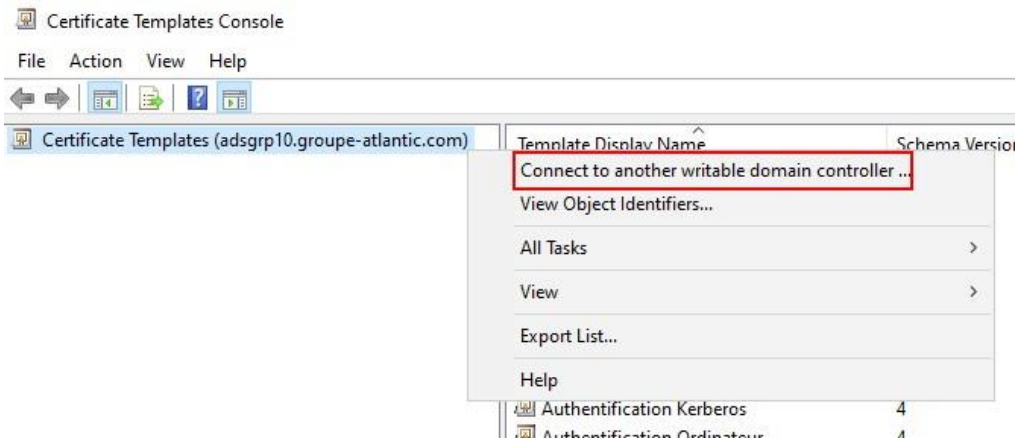


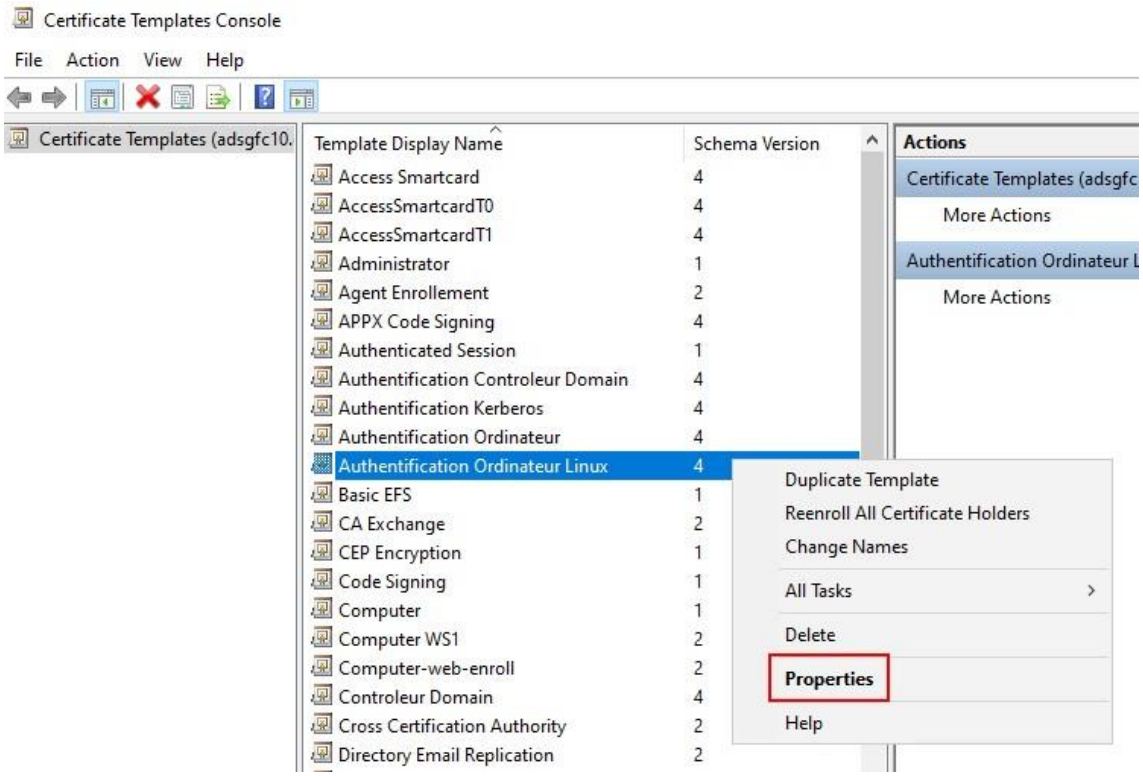


Check on which domain controller you're currently connected using powershell and the command : **getaddomaincontroller**

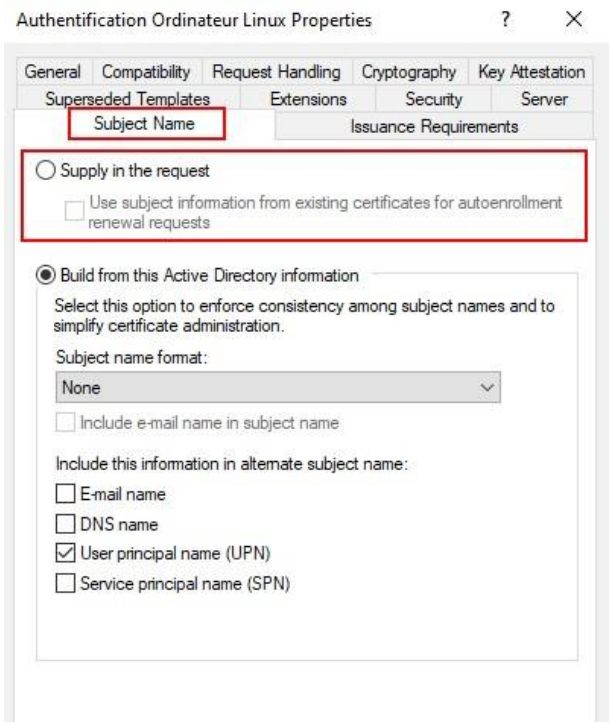


Make sur you are connecting to the same server on the PKI:

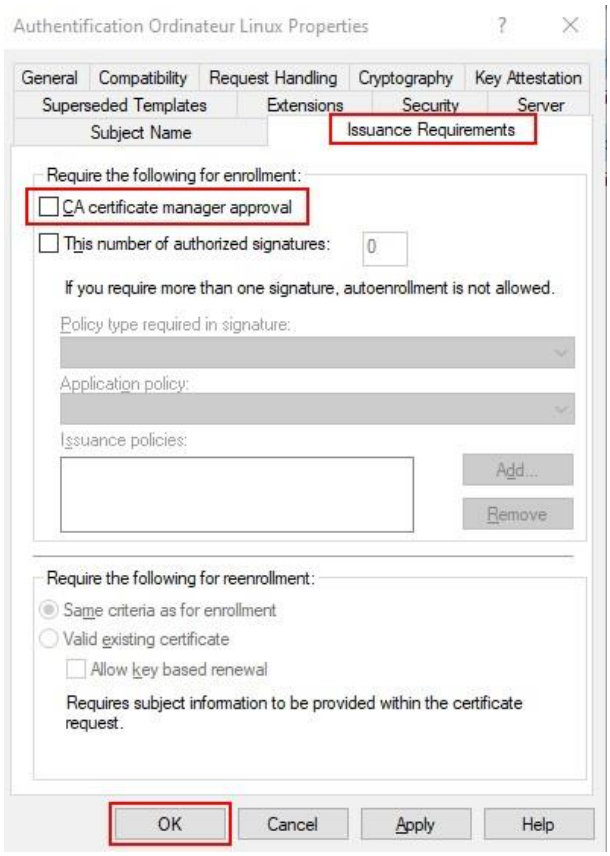




Select the option **Supply in the request**



Unselect the option **CA certificate manager approval**



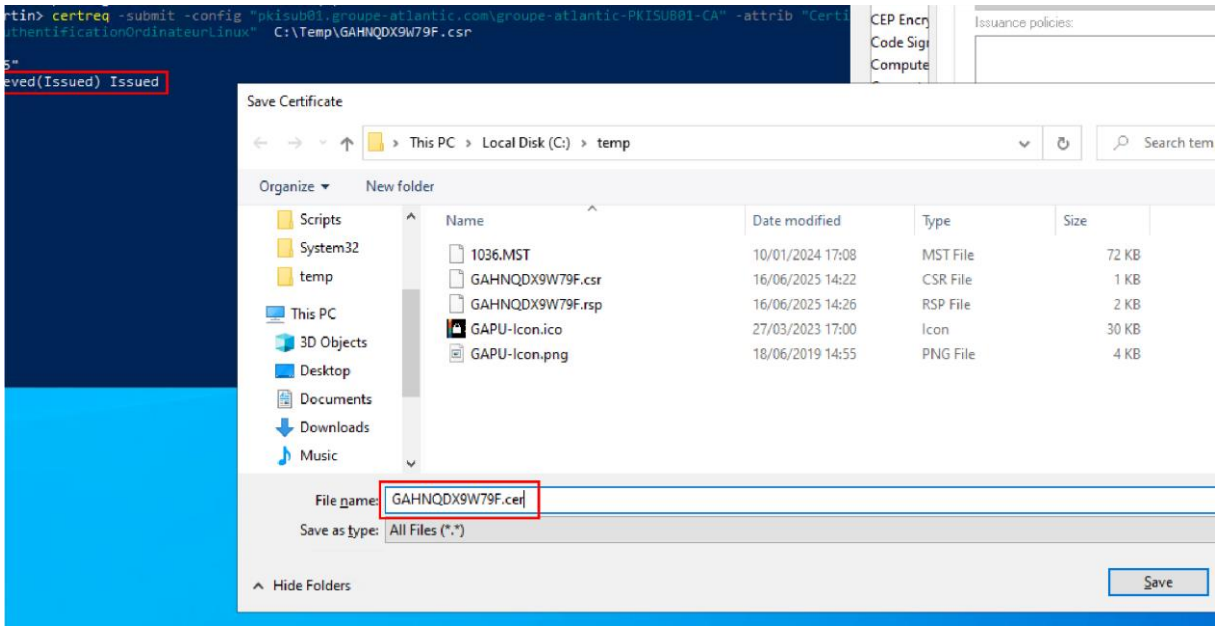
There can be a several minutes delay before the update is replicated to other domain controllers, otherwise the request will be pending.

Submit the certificate request

Copy the csr file in **C:\Temp**

Launch Powershell and type the following command:

certreq -submit -config "pkisub01.groupe-atlantic.com\groupe-atlantic-PKISUB01-CA" -attrib "Certificate Template:AuthentificationOrdinateurLinux" C:\Temp*xxx.csr*

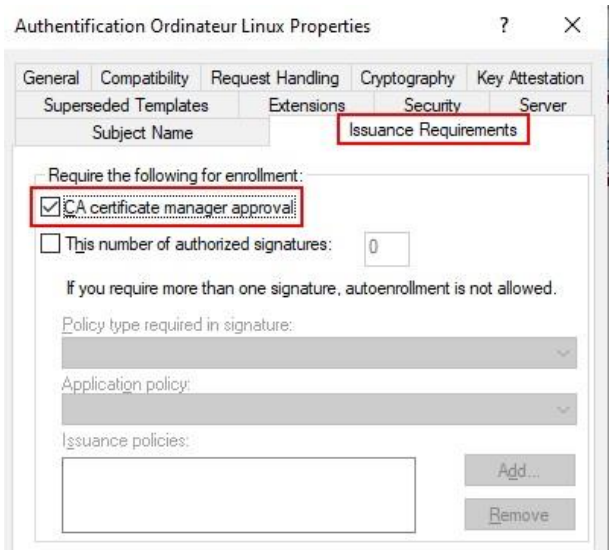


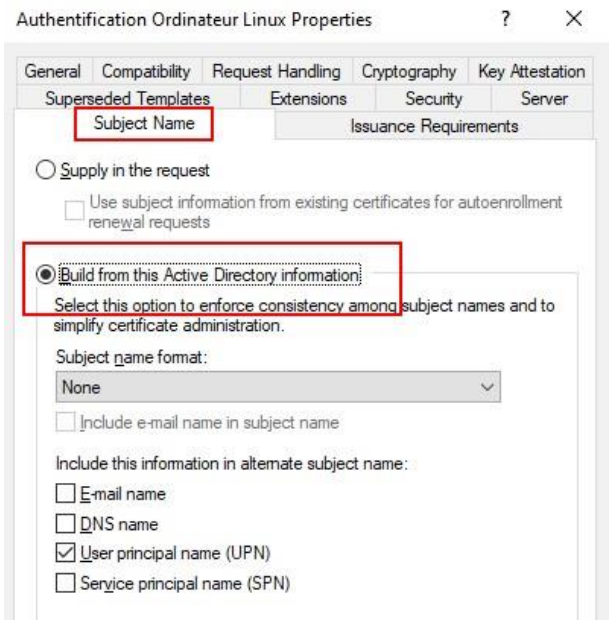
Save the file as **.crt** or **.cer** file and install it on the destination computer.

Template and files security

WARNING!

Configure the certificate back to its secure configuration:





Make sure you do not leave the cer/crt files in an unsecure place. **Do not store them**, they must be **removed** after the installation.