NETGEAR®

Manuel de l'utilisateur.

BE9400 Tri-bande PoE 2.5G Point d'accès Insight Managed Access Points WiFi 7 AX3000

WBE718

Mars 2026
202-12807-04

NETGEAR, Inc.

Support et communauté

Visitez https://www.netgear.com/fr/support/ pour obtenir des réponses à vos questions et accéder aux derniers téléchargements.

Vous pouvez également consulter notre communauté NETGEAR pour obtenir de bons conseils sur community.netgear.com.

Réglementation et aspects juridiques

Pour les informations à propos de la conformité réglementaire, y compris la Déclaration de conformité pour l'UE, rendez-vous sur https://www.netgear.com/fr/about/regulatory/.

Avant de brancher l'alimentation, reportez-vous au document de conformité légale.

Pour connaître la politique de confidentialité de NETGEAR, rendez-vous sur le site https://www.netgear.com/fr/about/privacy-policy/.

Lorsque la loi le permet, en utilisant cet appareil, vous acceptez les conditions générales de NETGEAR sur le site https://www.netgear.com/fr/about/terms-and-conditions et, si vous n'acceptez pas, retournez l'appareil à votre lieu d'achat pendant votre période de retour.

Ce produit est conçu et garanti pour une utilisation en intérieur uniquement. N'utilisez pas cet appareil à l'extérieur. La source PoE est destinée à une connexion à l'intérieur d'un bâtiment uniquement.

Applicable uniquement aux appareils 6 GHz : utilisez l'appareil en intérieur uniquement. L'utilisation d'appareils 6 GHz est interdite sur les plateformes pétrolières, les voitures, les trains, les bateaux et les aéronefs, à une exception : l'utilisation de cet appareil est autorisée sur les grands avions volant à plus de 10 000 pieds d'altitude. L'utilisation d'émetteurs dans les bandes 5,925-7,125 GHz est interdite pour le contrôle ou les communications avec des systèmes aériens de pilotage automatique.

Marques commerciales

© NETGEAR, Inc., NETGEAR et le logo NETGEAR sont des marques commerciales de NETGEAR, Inc. Toutes les marques commerciales autres que NETGEAR sont utilisées à des fins de référence uniquement.

Historique de révision

Numéro de pièce de publication	Date de publication	Commentaires
202-12807-04	Mars 2026	EN: 202-12734-07 Nous avons révisé les sections suivantes : • Connectez-vous via WiFi à l'interface utilisateur de l'appareil pour la configuration initiale à la page 37 • Connectez-vous sur le LAN à l'interface utilisateur du périphérique pour la configuration initiale à la page 42 • Configurez le AP hors ligne à l'aide d'un ordinateur directement connecté à la page 47 Nous avons ajouté les sections suivantes : • Échec DHCP de l'affichage à la page 300 Nous avons ajouté la configuration SNMPv3 : • Activez SNMP et gérez les paramètres SNMP à la page 272 • Configurez les paramètres SNMPv1/v2c à la page 274 • Configurez les paramètres SNMPv3.configurez les paramètres SNMPv3 à la page 275 Nous avons révisé les sections suivantes : • Configurez Multi PSK pour un réseau WiFi à la page 97 • Capturez les paquets WiFi et Ethernet à la page 362
202-12807-03	Mai 2025	EN: 202-12734-05 Nous avons ajouté les sections suivantes : • Gérer la protection contre les dénis de service à la page 217 • Configurez le mode de puissance d'entrée PoE à la page 282 Nous avons mis à jour les sections suivantes : • Configurez un réseau WiFi ouvert ou sécurisé à la page 73 • Activer ou désactiver le guidage de bande à la page 103 • Gérer la qualité de service pour une radio WiFi à la page 124 • Configurez un portail captif externe pour un réseau WiFi à la page 130 • Configurer les serveurs RADIUS à la page 143 • Gérer la détection des points d'accès voisins à la page 147 • Afficher la distribution des clients, les clients connectés et les tendances des clients à la page 296 • Afficher le volume de trafic, les informations sur les ventilateurs, les statistiques et l'utilisation des canaux à la page 302 • Paramètres par défaut à la page 382 Nous avons fait d'autres mises à jour et corrections mineures.

(A continué)

Numéro de pièce de publication	Date de publication	Commentaires
202-12807-02	Février 2025	EN: 202-12734-04 Nous avons ajouté les sections suivantes : • Bloquer des URL et des mots-clés spécifiques pour l'accès à Internet à la page 142 • Effectuez un test de débit à la page 366 Nous avons mis à jour les sections suivantes : • Voyants du panneau supérieur à la page 18 • Configurez Multi PSK pour un réseau WiFi à la page 97 • Configurez un portail captif externe pour un réseau WiFi à la page 130 • Configurer les serveurs RADIUS à la page 143 • Configurez un pont WiFi entre les points d'accès à la page 344
202-12807-01	Janvier 2025	EN: 202-12734-03 Première publication.

Sommaire

Chapitre 1 Introduction

Documentation supplémentaire..... 14
Comment gérer le AP..... 14
À propos de l'interface utilisateur du périphérique et du contrôleur NETGEAR engage..... 15
À propos de l'interface utilisateur du périphérique et de Netgear insight..... 16

Chapitre 2 Aperçu du matériel

Déballez le AP..... 18
Voyants du panneau supérieur..... 18
Interface matérielle..... 20
Etiquette produit..... 21
Consignes de sécurité et avertissements pour un point d'accès intérieur..... 22

Chapitre 3 Installez le AP sur votre réseau et accédez-y pour la configuration initiale

Positionnez votre AP pour obtenir des performances optimales. 26
Configurez et connectez le AP à votre réseau..... 27
Connectez-vous au AP pour la configuration initiale..... 29
Utilisez le contrôleur engage NETGEAR pour ajouter un point d'accès à un site engage..... 30
Connectez-vous sur Internet à l'aide du portail cloud Netgear insight..... 32
Connectez-vous via WiFi à l'aide de l'application Netgear insight..... 34
Connectez-vous via WiFi à l'interface utilisateur de l'appareil pour la configuration initiale..... 37
Connectez-vous sur le LAN à l'interface utilisateur du périphérique pour la configuration initiale..... 42
Configurez le AP hors ligne à l'aide d'un ordinateur directement connecté..... 47
Connectez-vous au AP après la configuration initiale..... 52
Informations d'identification de l'interface utilisateur du périphérique..... 53
Que faire si vous recevez un avertissement de sécurité du navigateur..... 56

Chapitre 4 Installez le AP sur un réseau WiFi maillé instantané Insight

Qu'est-ce qu'une racine et un nœud ?..... 60
Qu'est-ce qu'un réseau WiFi Insight instant Mesh ?..... 61
Conditions requises pour placer un nœud dans un réseau WiFi Insight instant Mesh..... 62
Accédez au portail Cloud pour configurer ou gérer un réseau WiFi Insight instant Mesh..... 63
Connectez APen tant que nœud à une racine à l'aide de Cloud Portal..... 63
Installez l'application Insight pour gérer un réseau WiFi maillé instantané Insight..... 66
Connectez APen tant que nœud à une racine à l'aide de l'application Insight..... 67

Chapitre 5 Gérer les fonctions WiFi de base d'un réseau WiFi

Configurez un réseau WiFi ouvert ou sécurisé..... 73
Afficher ou modifier les paramètres d'un réseau WiFi..... 84
Supprimer un réseau WiFi..... 86
Masquer ou diffuser le SSID d'un réseau WiFi..... 87
Modifiez l'ID VLAN d'un réseau WiFi..... 89
Modifier l'authentification et la sécurité d'un réseau WiFi..... 90
Activer ou désactiver PMF pour un réseau WiFi..... 96
Configurez Multi PSK pour un réseau WiFi..... 97
Activer ou désactiver un réseau WiFi ou configurer un programme d'activité WiFi..... 101
Activer ou désactiver le guidage de bande..... 103
Configurer l'opération multi-liens..... 105

Chapitre 6 Gérer les fonctions de base de la radio

Gérez les paramètres WiFi de base des radios..... 109
Permet d'allumer ou d'éteindre une radio..... 113
Permet de modifier le mode préambule d'une radio..... 114
Permet de changer de canal pour une radio..... 117
Modifier l'intervalle de garde d'une radio..... 119
Modifier la puissance de sortie d'une radio..... 121
Permet de changer de canal pour une radio..... 123
Gérer la qualité de service pour une radio WiFi..... 124

Chapitre 7 Configurer et gérer un portail captif

Configurez un portail captif accessible par clic pour un réseau WiFi..... 128
Configurez un portail captif externe pour un réseau WiFi..... 130

Chapitre 8 Gérer l'accès et la sécurité

Gérer les comptes utilisateur..... 136
Ajouter un compte utilisateur..... 136
Modifier le délai d'expiration d'une session utilisateur..... 138
Modifier les paramètres d'un compte utilisateur..... 139
Supprimer un compte utilisateur..... 140
Bloquer des URL et des mots-clés spécifiques pour l'accès à Internet..... 142
Configurer les serveurs RADIUS..... 143
Gérer la détection des points d'accès voisins..... 147
Activez la détection des points d'accès voisins et déplacez les points d'accès vers la liste des points d'accès connus..... 148
Importez une liste de points d'accès voisins existante dans la liste des points d'accès connus..... 150
Gérez les listes de contrôle d'accès MAC globales et les stratégies de trafic..... 152
Listes de contrôle d'accès MAC globales pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé..... 153
Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé..... 154
Importez une ACL MAC existante pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé..... 156
Bloquez tout le trafic de diffusion et de multidiffusion à partir du réseau local filaire..... 158
Gérer le filtre antibruit sans fil..... 159
Activez ou désactivez le filtre antibruit sans fil..... 160
Activez, désactivez ou modifiez une règle de trafic dans le filtre antibruit sans fil..... 161
Modifiez la priorité d'une règle de trafic dans le profil application QoS..... 166
Gérer le filtre de trafic global..... 167
Activez ou désactivez le filtre de trafic global..... 168
Ajoutez une règle de trafic au filtre de trafic global..... 169
Modifiez une règle de trafic dans le filtre de trafic global. 173
Modifiez la priorité d'une règle de trafic dans le filtre de trafic global..... 175
Supprimez une règle de trafic du filtre de trafic global.... 176
Gérer l'ordre de priorité du trafic..... 177
Gérer le profil de trafic application QoS..... 178
Activez, désactivez ou modifiez une règle de trafic dans le profil application QoS..... 178
Activez ou désactivez le profil application QoS..... 180

Modifiez la priorité d'une règle de trafic dans le profil application QoS..... 182
Gérer le profil de règle globale..... 183
Ajouter, modifier ou supprimer une règle du profil règle globale..... 183
Activer ou désactiver le profil règle globale..... 186
Modifiez la priorité d'une règle de trafic dans le profil règle globale..... 188
Gérez les listes de contrôle d'accès MAC basées sur SSID et les stratégies de trafic pour les réseaux WiFi..... 189
Gérer les listes de contrôle d'accès MAC pour les clients WiFi..... 190
Configurez manuellement une ACL MAC pour les clients WiFi..... 191
Importez une ACL MAC existante pour les clients WiFi.... 194
Listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi..... 198
Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi..... 199
Importez une liste de contrôle d'accès MAC existante pour le trafic de diffusion et de multidiffusion à partir de clients WiFi..... 202
Gérer les groupes de filtres de trafic MAC/IP pour les réseaux WiFi..... 205
Activer ou désactiver un groupe de filtres de trafic MAC/IP..... 205
Ajoutez une règle de trafic à un groupe de filtres de trafic MAC/IP..... 207
Modifier une règle de trafic dans un groupe de filtres de trafic MAC/IP..... 211
Modifiez la priorité d'une règle de trafic dans un groupe de filtres de trafic MAC/IP..... 213
Supprimez une règle de trafic d'un groupe de filtres de trafic MAC/IP..... 214
Activer la sécurité L2..... 215
Gérer la protection contre les dénis de service..... 217

Chapitre 9 Gérer le réseau local et les paramètres IP

Désactivez le client DHCP et définissez une adresse IP fixe..... 221
Activez le client DHCP..... 222
Définissez le VLAN de gestion et de VLAN 802.1Q..... 224
Définissez un nom de domaine existant..... 226
Activer ou désactiver le protocole Spanning Tree..... 227

Activer ou désactiver la fonction de vérification de l'intégrité du réseau..... 229
Activer ou désactiver igmp snooping..... 230
Activer ou désactiver le chemin de données assisté par matériel..... 231
Activer ou désactiver Ethernet LLDP..... 233
Activer ou désactiver UPnP..... 234
Gérer la passerelle DNS multicast..... 235
Activez la passerelle DNS de multidiffusion et ajoutez une stratégie..... 236
Modifier ou supprimer une stratégie DNS de multidiffusion. 239

Chapitre 10 Gérer et entretenir le AP

Changez le mode de gestion en Netgear insight ou navigateur Web..... 242
Modifiez le pays ou la région d'exploitation..... 244
Modifiez le mot de passe du compte utilisateur admin..... 246
Modifiez le nom du système..... 247
Spécifiez un serveur NTP personnalisé..... 248
Définissez le fuseau horaire..... 250
Gérer les paramètres syslog..... 251
Gérer le micrologiciel du AP..... 253
Laissez le AP rechercher un nouveau micrologiciel et mettez-le à jour..... 254
Téléchargez manuellement le micrologiciel et mettez à jour le AP..... 256
Revenez au micrologiciel de sauvegarde..... 258
Utilisez un serveur SFTP pour mettre à jour AP..... 260
Gérer le fichier de configuration du AP..... 262
Sauvegardez la configuration :..... 262
Restaurez la AP configuration..... 264
Utilisez le bouton Réinitialiser pour redémarrer le AP..... 266
Redémarrez APà partir de l'interface utilisateur du périphérique..... 266
Programmez le redémarrage duAP..... 267
Rétablissez les paramètres par défaut du routeur..... 269
Utilisez le bouton DE RÉINITIALISATION pour réinitialiser le commutateur AP..... 270
Utilisez l'interface utilisateur du périphérique pour réinitialiser le commutateur AP..... 270
Activez SNMP et gérez les paramètres SNMP..... 272
Configurez les paramètres SNMPv1/v2c..... 274
Configurez les paramètres SNMPv3.configurez les paramètres SNMPv3..... 275

Gérer la LED..... 279
Gérer le mode efficacité énergétique..... 280
Configurez le mode de puissance d'entrée PoE..... 282

Chapitre 11 Surveillez le AP et le réseau

Affiche les APparamètres Internet, IP et système..... 285
Afficher les paramètres radio WiFi..... 288
Afficher les points d'accès voisins inconnus et connus..... 291
Afficher les statistiques des stratégies de trafic MAC et IP..... 293
Afficher la distribution des clients, les clients connectés et les tendances des clients..... 296
Échec DHCP de l'affichage..... 300
Afficher le volume de trafic, les informations sur les ventilateurs, les statistiques et l'utilisation des canaux..... 302
Afficher ou télécharger les URL suivies..... 306
Affichez, enregistrez, téléchargez ou effacez les journaux..... 308
Afficher une connexion de pont WiFi..... 310
Afficher les alarmes et les notifications..... 311

Chapitre 12 Gérer les fonctions WiFi avancées d'un réseau WiFi

Définissez le mode NAT ou Bridge pour l'adressage et le trafic. 315
Activer ou désactiver l'isolation client pour un réseau WiFi..... 317
Activer ou désactiver le suivi d'URL pour un réseau WiFi..... 320
Sélectionnez une liste de contrôle d'accès MAC pour les clients WiFi dans un réseau WiFi..... 321
Définissez des limites de débit de bande passante pour un réseau WiFi..... 324
Modifier le format des messages d'offre DHCP dans un réseau WiFi..... 326
Sélectionnez une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi dans un réseau WiFi..... 328
Bloquez tout trafic de diffusion et de multidiffusion pour un réseau WiFi..... 330
Sélectionnez un groupe de filtres de trafic MAC/IP pour un réseau WiFi..... 332
Configurer la sélection avancée du débit pour un réseau WiFi. 334
Attribuez des noms d'hôte aux clients WiFi et gérez la liste des noms d'hôte..... 338

Chapitre 13 Configurez un pont WiFi dans un système de distribution sans fil

Exigences relatives à la station de base Wi-Fi, au répéteur Wi-Fi et au pont Wi-Fi..... 342

Configurez un pont WiFi entre les points d'accès..... 344

Chapitre 14 Gérer les fonctions avancées de la radio

Gérez les paramètres WiFi avancés des radios..... 348
Gérer le nombre maximal de clients pour une radio..... 351
Permet de gérer les paramètres de diffusion et de multidiffusion d'une radio..... 352
Gérer l'équilibrage de charge des radios..... 354
Gérez les clients collants..... 357
Gérer le proxy ARP..... 359

Chapitre 15 Diagnostics et dépannage

Capturez les paquets WiFi et Ethernet..... 362
Effectuez un test ping..... 364
Effectuez un test de débit..... 366
Conseils rapides pour le dépannage WiFi..... 367
Dépanner avec les voyants..... 369
Le voyant reste éteint..... 369
Le voyant reste orange fixe..... 370
Le AP fonctionne comme un PoE PD et le voyant clignote en vert en continu..... 371
Le voyant clignote en orange lentement et en continu..... 371
Le voyant ne s'allume pas en bleu en mode de gestion Netgear insight..... 372
Le voyant ne cesse pas de clignoter en orange, vert et bleu. 373
Le nœud et la racine ne peuvent pas se connecter..... 374
Dépannez la connectivité WiFi pour un client WiFi..... 375
Dépannage de la navigation Internet..... 376
Vous ne pouvez pas vous connecter à APvia une connexion LAN..... 377
Les modifications ne sont pas enregistrées..... 378
Vous entrez un mot de passe incorrect et ne pouvez plus vous connecter à AP..... 378
Dépannez votre réseau à l'aide de l'utilitaire ping..... 379
Testez le chemin LAN vers votre routeur AP..... 379
Tester le chemin de votre ordinateur vers un périphérique distant..... 380

Annexe A Paramètres usine par défaut et caractéristiques techniques

Paramètres par défaut..... 382
Caractéristiques techniques..... 387

1

Introduction

Ce manuel est destiné au Insight point d'accès Wifi 7 managé PoE 2.5G Tri-bande NETGEAR BE9400 modèle WBE718.

Le modèle WBE718, appelé dans ce manuel AP, prend en charge la norme Wi-Fi 7 avec IEEE 802.11be, quatre flux de données (2+2) et un fonctionnement simultané tribande à 6 GHz, 5 GHz et 2,4 GHz, permettant un débit combiné d'environ 9,4 Gbit/s (5765 Mbit/s à 6 GHz, 2882 Mbit/ s à 5 GHz et 688 Mbit/s à 2,4 GHz).

Le AP peut fonctionner comme un périphérique alimenté par alimentation par Ethernet plus (PoE+, 802.3at) dans un réseau existant connecté à un commutateur PoE+. Le APprend également en charge un adaptateur secteur pour la connexion à un commutateur ou routeur standard. Le port Ethernet PoE+ prend en charge des vitesses de 100 Mbit/s, 1 Gbit/s et 2,5 Gbit/s.

Ce chapitre comprend les sections suivantes :

- Documentation supplémentaire
- Comment gérer le AP
- À propos de l'interface utilisateur du périphérique et du contrôleur NETGEAR engage
- À propos de l'interface utilisateur du périphérique et de Netgear insight

REMARQUE: Pour plus d'informations sur les sujets traités dans ce manuel, visitez le site Web d'assistance à l'adresse netgear.com/support .

REMARQUE: Des mises à jour du micrologiciel avec de nouvelles fonctionnalités et des corrections de bugs sont disponibles de temps à autre sur netgear.com/support/download/. Vous pouvez rechercher et télécharger manuellement un nouveau micrologiciel. Si les fonctionnalités ou le comportement de votre produit ne correspondent pas aux éléments décrits dans ce manuel, il peut être nécessaire de procéder à la mise à jour de votre micrologiciel (firmware).

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Documentation supplémentaire

Les documents suivants sont disponibles à l ' adresse suivante : netgear.com/support/download/:

- Guide d'installation
- Guide d'installation et de fixation WiFi Pro
- Fiche technique

AP La gestion via le contrôleur d'engagement NETGEAR est décrite dans le manuel d'utilisation du contrôleur d'engagement, également disponible à l'adresse netgear.com/support/download/.

AP La gestion dans Netgear insight est décrite dans la base de connaissances NETGEAR. Voir kb.netgear.com/000044338/.

Comment gérer le AP

Si vous utilisez le contrôleur NETGEAR engage pour gérer un réseau, vous pouvez laisser le contrôleur intégré au APpour configurer et gérer le AP.

Pour les abonnés NETGEAR Insight Premium et Insight Pro, le switch prend en charge le portail NETGEAR Insight Cloud et l'application NETGEAR Insight.

- **Portail Insight Cloud**. Vous pouvez détecter et gérer le PA sur le portail de la plateforme de gestion dans le cloud Insight.
- Application Insight Vous permet de configurer et de gérer APà partir de votre appareil mobile iOS ou Android et se connecte à la plate-forme de gestion basée sur le cloud Insight.

Vous pouvez également gérer APavec l'interface utilisateur du terminal. La gestion via la plate-forme de gestion basée sur le cloud Insight ou le contrôleur engage et la gestion via l'interface utilisateur de l'appareil sont mutuellement exclusives. En outre, Netgear insight et le contrôleur d'engagement sont des méthodes de gestion mutuellement exclusives.

Vous pouvez gérer et surveiller le AP à l'aide des méthodes suivantes :

- **Gestion engage uniquement** : Vous utilisez uniquement le contrôleur d'engagement. Toutefois, si vous le souhaitez, vous pouvez à tout moment passer à la méthode de gestion autonome.
- **Gestion Insight uniquement** : Vous utilisez uniquement le portail cloud Insight ou l'application Insight. Toutefois, si vous le souhaitez, vous pouvez à tout moment passer à la méthode de gestion autonome.
- Gestion autonome Vous utilisez APen tant que périphérique autonome dans votre réseau et gérez et surveillez APuniquement à l'aide de l'interface utilisateur du périphérique. Il s'agit de la méthode de gestion par défaut. Toutefois, si vous le souhaitez, vous pouvez à tout moment passer à la méthode de gestion engage-Only ou Insight-Only.

À propos de l'interface utilisateur du périphérique et du contrôleur NETGEAR engage

Ce manuel de l'utilisateur décrit APl'interface utilisateur du terminal de et les tâches que vous pouvez effectuer à l'aide de l'interface utilisateur du terminal.

Si vous installez APen tant que terminal géré par le contrôleur engage, les paramètres des fonctionnalités que vous pouvez gérer via le contrôleur engage sont masqués dans l'interface utilisateur du terminal. Cependant, à l'aide de l'interface utilisateur du périphérique, vous pouvez toujours gérer les paramètres de certaines fonctionnalités. En outre, les tâches de surveillance, de maintenance et de diagnostic restent disponibles dans l'interface utilisateur du périphérique.

Ce manuel ne décrit pas les procédures relatives au contrôleur engagement NETGEAR, qui sont documentées dans le manuel d'utilisation du contrôleur engagement, que vous pouvez télécharger sur le site netgear.com/support/download/. Une exception est la section suivante : Utilisez le contrôleur engage NETGEAR pour ajouter un point d'accès à un site engage à la page 30.

Pour plus d'informations sur le mot de passe requis pour accéder à l'interface utilisateur du terminal lorsque APest géré par le contrôleur d'engagement, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

À propos de l'interface utilisateur du périphérique et de Netgear insight

Ce manuel d'utilisation décrit l'interface utilisateur du périphérique, que vous utilisez si APfonctionne comme un point d'accès autonome.

Pour plus d'informations sur les abonnements Netgear insight, visitez netgear.com/business/services/insight/ et kb.netgear.com/000061848.

Ce manuel ne décrit pas les procédures Netgear insight, qui sont documentées dans la base de connaissances NETGEAR. Pour obtenir des articles de la base de connaissances sur Netgear insight, visitez le site kb.netgear.com/000044338/.

Si vous installez APen tant que terminal géré par Netgear insight, les paramètres des fonctionnalités que vous pouvez gérer via le portail cloud Insight et l'application Insight sont masqués dans l'interface utilisateur du terminal. Cependant, à l'aide de l'interface utilisateur du terminal, vous pouvez toujours gérer les paramètres de certaines fonctionnalités qui ne sont pas encore prises en charge dans Insight. En outre, les tâches de surveillance, de maintenance et de diagnostic restent disponibles dans l'interface utilisateur du périphérique.

Pour plus d'informations sur le mot de passe requis pour accéder à l'interface utilisateur du terminal lorsque APest géré par Netgear insight, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

2

Aperçu du matériel

Le point d'accès Wifi 7 géré Insight PoE 2.5G NETGEAR BE9400 est un point d'accès *intérieur*.

Ce chapitre contient les sections suivantes :

- Déballez le AP
- Voyants du panneau supérieur
- Interface matérielle
- Etiquette produit
- Consignes de sécurité et avertissements pour un point d'accès intérieur

Déballez le AP

L'emballage doit contenir les éléments suivants :

- WBE718 AP avec le couvercle de port fixé
- Plaque de fixation [La taille réglable est réglée sur la position « P1 ».]
- Clip profond
- Clip peu profond
- Guide d'installation

REMARQUE: Selon le produit commandé, il est possible que l'emballage ne comprenne pas d'adaptateur secteur. Pour mettre le sous tensionAP, connectez-le à un commutateur PoE+. Si vous avez commandé un paquet sans adaptateur secteur, vous pouvez toujours commander un adaptateur secteur en option.

Pour plus d'informations sur les différentes options de montage, consultez le *Guide d'installation du support Pro WiFi* , que vous pouvez télécharger sur le site netgear.com/support/download/.

Voyants du panneau supérieur

Le voyant qui fournit l'état du APse trouve sur le bord du panneau supérieur du AP.

Illustration 1 : Panneau supérieur avec LED

Table 1 : Description des voyants

Couleur		Description
Comportement normal		
	Désactivé	Aucune alimentation n'est fournie au AP.
	Orange fixe, temporairement	le PA est en cours de démarrage ou le bouton de réinitialisation a été activé.
	Violet continu	Le PA est en cours d'initialisation.
	Magenta clignotant, lentement	L' AP continue à s'initialiser.
	Orange clignotant rapidement, temporairement	Le APmet à jour le micrologiciel ou réinitialise les paramètres par défaut.
	Bleu continu	Le PA fonctionne en mode Insight et est connecté à la plateforme d'administration cloud Insight.
	Vert fixe	Le point d'accès a démarré et fonctionne comme point d'accès autonome ou comme point d'accès détecté par Insight non connecté à la plateforme de gestion cloud Insight.
	Bleu clignotant :	Au moins un client WiFi est connecté au AP. La vitesse de clignotement dépend du débit de transmission et de réception des données des clients connectés.
	Multicolore clignotant	Le APfonctionne comme un nœud dans un réseau WiFi maillé instantané Insight et la configuration du maillage est en cours.
Indication du problème		
	Vert clignotant, en continu	La puissance PoE que reçoit le APn'est pas au niveau PoE++ (802.3at3bt) requis.

Table 1 : Description des voyants (A continué)

Couleur		Description
	Clignotement orange lent, continu	Le APn'a pas reçu d'adresse IP d'un serveur DHCP.
	Orange fixe, en continu	Une erreur de démarrage s'est produite ou le APfonctionne mal.

REMARQUE: Pour plus d'informations sur le dépannage de la LED, reportez-vous à la section Dépanner avec les voyants à la page 369.

Interface matérielle

Le panneau inférieur du APest doté d'un port LAN/PoE+, d'un connecteur d'alimentation CC pour un adaptateur secteur en option et d'un bouton de **réinitialisation**.

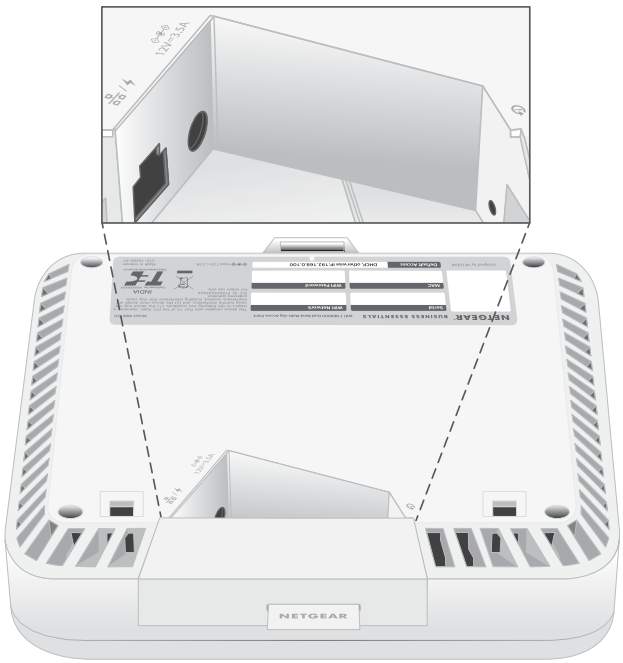

Illustration 2 : Interface matérielle

Le panneau inférieur contient les composants suivants, illustrés de gauche à droite dans la figure précédente :

- Port LAN/PoE+ Vous pouvez utiliser le port LAN/PoE+ 2.5G RJ-45 pour connecter le AP à un commutateur PoE+ (802.3at) ou, si vous utilisez un adaptateur secteur en option, à un commutateur non PoE.

  Lorsqu'il est connecté aux équipements 2,5 Gbit/s, le port WAX620 LAN PoE+ prend en charge les vitesses Ethernet jusqu'à 2,5 Gbit/s au sein de votre réseau local. Si votre connexion Internet, votre modem, votre routeur et votre switch prennent en charge une vitesse de 2,5 Gbit/s, la connexion Internet du PA fonctionne également à 2,5 Gbit/s. Sinon, la connexion Internet fonctionne à la vitesse la plus élevée prise en charge par votre connexion FAI, modem, routeur et commutateur.

  Pour plus d'informations sur la connexion du port LAN/PoE+, reportez-vous à la section Configurez et connectez le AP à votre réseau à la page 27.

- **Connecteur d'alimentation CC**. Si vous n'utilisez pas de commutateur PoE+ pour alimenter le AP, connectez un adaptateur secteur en option au connecteur d'alimentation CC.

- Bouton **Reset** (Réinitialiser) : Vous pouvez utiliser le bouton **Réinitialiser** pour redémarrer le AP ou pour rétablir les paramètres par défaut du AP:

  - Redémarrer le système Pour redémarrer le AP, appuyez sur le bouton de **réinitialisation** pendant environ deux secondes jusqu'à ce que le voyant s'allume en orange fixe, puis relâchez immédiatement le bouton. Pour plus d'informations, consultez la section Utilisez le bouton Réinitialiser pour redémarrer le AP à la page 266.
  - Reset (Réinitialiser) Pour rétablir les paramètres par défaut duAP, appuyez sur le bouton **de réinitialisation** jusqu'à ce que le voyant clignote en orange, après quoi vous pouvez relâcher le bouton. Pour plus d'informations, consultez la section Utilisez le bouton DE RÉINITIALISATION pour réinitialiser le commutateur AP à la page 270.

    Si vous maintenez le bouton de **réinitialisation** enfoncé, le voyant s'allume d'abord en orange fixe, puis clignote en orange environ 5 secondes plus tard. Si vous relâchez le bouton alors que le voyant est orange fixe, le AP redémarre au lieu de se réinitialiser. Le voyant doit clignoter en orange.

Etiquette produit

L'étiquette du produit APindique le code QR, le numéro de série, l'adresse MAC, le nom du réseau WiFi (SSID) de configuration et la clé réseau (mot de passe) du AP, ainsi

que l'adresse IP par défaut, le nom d'utilisateur par défaut et le mot de passe par défaut pour accéder à l'interface utilisateur du périphérique.

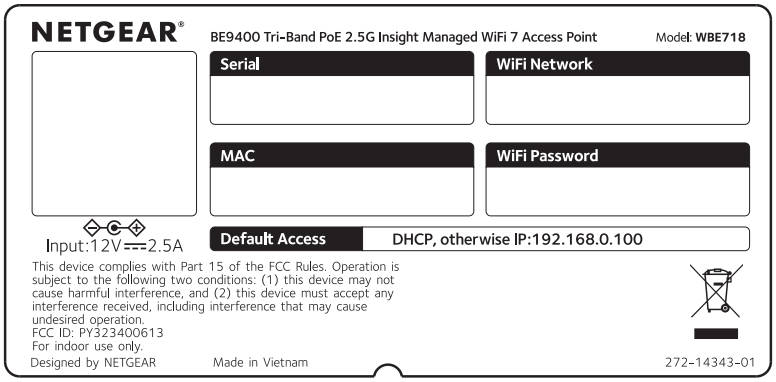

Illustration 3 : Etiquette produit

Consignes de sécurité et avertissements pour un point d'accès intérieur

Suivez ces consignes de sécurité pour assurer votre sécurité personnelle et protéger votre système contre les dommages potentiels :

Pour réduire les risques de blessures corporelles, d'électrocution, d'incendie et d'endommagement de l'équipement, observez les précautions suivantes :

- Ce produit est conçu pour une utilisation en intérieur uniquement dans un environnement à température et humidité contrôlées. Notez ce qui suit :
  - Pour plus d'informations sur l'environnement dans lequel ce produit doit fonctionner, reportez-vous aux spécifications environnementales en annexe ou à la fiche technique.
  - Si vous souhaitez le connecter à un appareil se trouvant à l'extérieur, ce dernier doit être correctement mis à la terre et protégé contre les surtensions. Vous devez également installer un dispositif Ethernet de protection contre les surtensions en ligne entre le switch et l'appareil extérieur. Le non-respect de cette consigne peut endommager le routeur.
  - avant de connecter ce switch à des câbles ou périphériques d'extérieur, lisez l'article https://kb.netgear.com/fr/000057103 pour obtenir des informations relatives à la confidentialité et à la garantie.

Le non-respect de ces directives peut entraîner des dommages à votre produit NETGEAR, qui pourraient ne pas être couverts par la garantie NETGEAR, dans la mesure permise par la loi applicable.

- Ne procédez à aucune intervention sur un produit, sauf dans les cas décrits dans la documentation de votre système. Certains appareils ne doivent jamais être ouverts.
- Si l'une des conditions suivantes se produit, débranchez le produit de la prise secteur, puis remplacez la pièce ou contactez votre fournisseur de services qualifié :
  - Selon votre produit, l'adaptateur secteur, le câble de l'adaptateur secteur, la fiche de l'adaptateur secteur ou le câble Ethernet PoE est endommagé.
  - Un objet est tombé dans le produit.
  - Le produit a été exposé à l'eau.
  - Le produit est tombé ou a été endommagé.
  - Le produit ne fonctionne pas correctement lorsque vous suivez les instructions d'utilisation.
- Tenez le produit à l'écart des radiateurs et des sources de chaleur. Ne bloquez pas non plus les évents de refroidissement.
- Ne renversez pas d'aliments ou de liquides sur les composants de votre produit et n'utilisez jamais le produit dans un environnement humide. Si le produit est mouillé, reportez-vous à la section appropriée de votre guide de dépannage ou contactez votre fournisseur de services qualifié.
- Ne poussez aucun objet dans les ouvertures de votre produit. Vous risqueriez de provoquer un incendie ou une électrocution en court-circuitant les composants intérieurs.
- Utilisez le produit uniquement avec un équipement approuvé.
- Le cas échéant, laissez-le refroidir avant de retirer les capots ou de toucher les composants internes.
- Assurez-vous que les périphériques connectés via des câbles Ethernet sont conçus pour fonctionner avec la puissance disponible sur votre site.
- En fonction de votre produit, utilisez uniquement l'adaptateur secteur fourni ou un câble Ethernet compatible PoE.

  Si votre produit utilise un adaptateur secteur :
  - Si vous n'avez pas reçu d'adaptateur secteur, contactez votre revendeur NETGEAR local.
  - L'adaptateur secteur doit être adapté au produit et à la tension et au courant indiqués sur l'étiquette des caractéristiques électriques du produit.
- Pour éviter tout risque d'électrocution, branchez les câbles d'alimentation du système et des périphériques sur des prises de courant correctement mises à la terre.

- Le cas échéant, les câbles d'alimentation des périphériques sont équipés de fiches à trois broches pour garantir une mise à la terre correcte. N'utilisez pas d'adaptateurs pour prises et ne retirez pas la broche de terre d'un câble. Si vous devez utiliser une rallonge, utilisez un câble à trois fils avec des fiches correctement mises à la terre.
- Respectez les valeurs nominales de la rallonge et de la barrette d'alimentation. Assurez-vous que l'ampérage total de tous les produits branchés sur le câble d'extension ou la multiprise ne dépasse pas 80 % de la limite d'ampérage pour le câble d'extension ou la multiprise.
- Pour protéger votre système contre les augmentations et les diminutions soudaines et transitoires de l'alimentation électrique, utilisez un parasurtenseur, un conditionneur de ligne ou un onduleur.
- Positionnez soigneusement les câbles du système, les câbles de l'adaptateur d'alimentation et les câbles Ethernet PoE. Acheminez les câbles de manière à ce qu'ils ne puissent pas être piétinés ou trébuchés. Assurez-vous que rien ne repose sur les câbles.
- Ne modifiez pas les adaptateurs d'alimentation, les câbles d'adaptateur d'alimentation, les câbles d'alimentation ou les fiches. Consultez un électricien agréé ou votre compagnie d'électricité pour toute modification du site.
- Respectez toujours les règles de câblage locales et nationales.

3

Installez le AP sur votre réseau et accédez-y pour la configuration initiale

Ce chapitre décrit comment installer et accéder à APsur votre réseau.

Ce chapitre contient les sections suivantes :

- Positionnez votre AP pour obtenir des performances optimales
- Configurez et connectez le AP à votre réseau
- Connectez-vous au AP pour la configuration initiale
- Connectez-vous au AP après la configuration initiale
- Informations d'identification de l'interface utilisateur du périphérique
- Que faire si vous recevez un avertissement de sécurité du navigateur

ATTENTION: Cet appareil doit être installé de façon professionnelle. Il est de la responsabilité de l'installateur de suivre les réglementations locales du pays, y compris les opérations au sein de canaux de fréquences, puissance de sortie et exigences DFS légaux. Le fournisseur, le revendeur ou le distributeur ne sont pas responsables des fonctionnements WiFi illégaux. Pour plus de détails, consultez les conditions générales de l'appareil.

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Positionnez votre AP pour obtenir des performances optimales

Avant d'installer et de monter votre AP comme décrit dans le guide d'installation ou dans une annexe de ce manuel, réfléchissez à la manière dont vous pouvez positionner le AP pour obtenir des performances optimales.

Les clients WiFi qui se trouvent à APportée WiFi peuvent se connecter au réseau WiFi. Cependant, la portée WiFi peut varier considérablement en fonction de l'emplacement physique de votre AP. Par exemple, l'épaisseur, la densité et le nombre de murs traversés par le signal WiFi peuvent limiter la portée.

En outre, d'autres périphériques WiFi dans et autour de votre bureau, maison, cour ou campus peuvent affecter le APsignal de votre. Les périphériques WiFi peuvent être d'autres points d'accès, routeurs, répéteurs, répéteurs WiFi et tout autre périphérique émettant des signaux WiFi pour fournir un accès réseau.

Conseils pour positionner votre AP:

- Placez votre AP près du centre de la zone où fonctionnent les clients WiFi.

  Il n'est pas nécessaire de disposer d'une visibilité directe entre le AP et les clients WiFi pour obtenir de bonnes performances.
- Si vous utilisez un adaptateur secteur, assurez-vous que le AP se trouve à portée d'une prise secteur.
- Placez le AP dans un endroit surélevé, en minimisant le nombre de murs et de plafonds entre le AP et les clients WiFi.
- Éloignez le routeur des périphériques électriques tels que :
  - Ventilateurs de plafond
  - Systèmes de sécurité à domicile
  - Micro-ondes
  - Ordinateurs
  - Bases de téléphones sans fil
  - Téléphones sans fil 2.4 GHz et 5,8 GHz
- Placez le routeur à l'écart des grandes surfaces métalliques, des grandes surfaces en verre, des murs isolés et des éléments tels que :
  - Portes métalliques pleines
  - Goujons en aluminium
  - Réservoirs de poisson

- Miroirs
- Brique
- Béton

Si vous utilisez APdes s autonomes adjacents, utilisez des canaux de radiofréquence sans chevauchement pour réduire les interférences. Pour plus d'informations, consultez la section Permet de changer de canal pour une radio à la page 123.

Configurez et connectez le AP à votre réseau

Vous pouvez connecter le AP à un commutateur Power over Ethernet plus (PoE+, 802.3at) de votre réseau. Le commutateur doit être connecté à un routeur réseau connecté à Internet. Si vous utilisez une connexion PoE++, le AP ne nécessite pas d'adaptateur secteur.

REMARQUE: Selon le produit commandé, il est possible que l'emballage ne comprenne pas d'adaptateur secteur. Pour mettre le sous tensionAP, connectez-le à un commutateur PoE++. Si vous avez commandé un pack sans adaptateur secteur mais que vous ne souhaitez pas utiliser une connexion PoE++, vous pouvez toujours commander un adaptateur secteur en option.

Lorsqu'il est connecté aux équipements 2,5 Gbit/s, le port WAX620 LAN PoE+ prend en charge les vitesses Ethernet jusqu'à 2,5 Gbit/s au sein de votre réseau local. Les figures précédentes montrent un switch NETGEAR MS510TXUP prenant en charge des vitesses jusqu'à 2,5 Gbit/s et supérieures, ainsi que le PoE++. Si votre connexion Internet, votre modem, votre routeur et votre switch prennent en charge une vitesse de 2,5 Gbit/s, la connexion Internet du PA fonctionne également à 2,5 Gbit/s. Sinon, la connexion Internet fonctionne à la vitesse la plus élevée prise en charge par votre connexion FAI, modem, routeur et commutateur.

La figure suivante illustre le APconnecté à un commutateur PoE++, qui dispose d'une connexion redondante à un routeur réseau connecté à Internet.

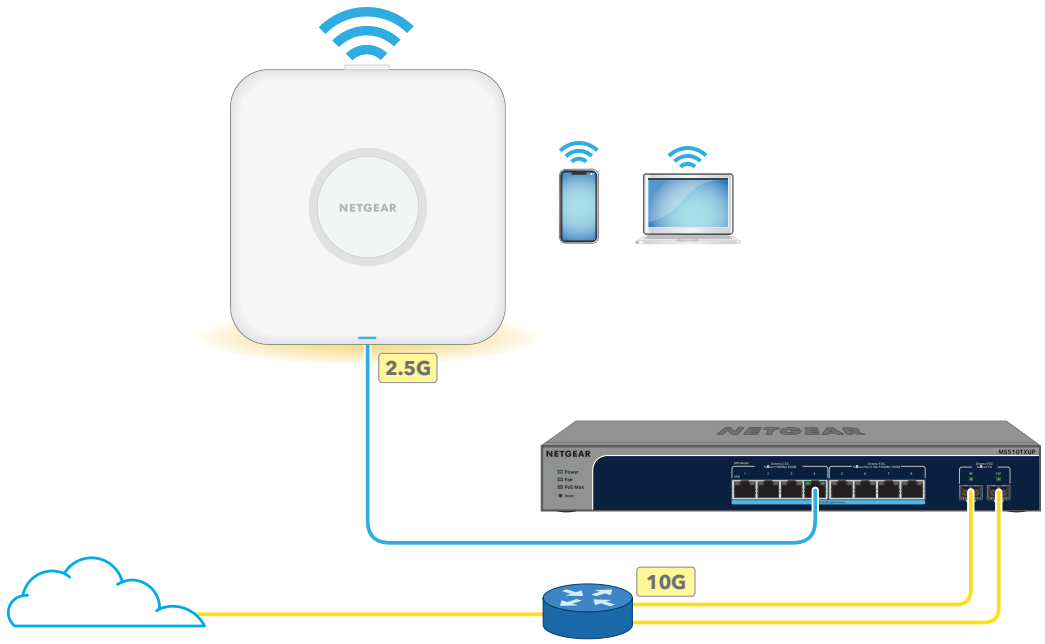

Illustration 4 : Configurez le AP avec une connexion PoE++ à votre réseau

Pour configurer le AP avec une connexion Ethernet à votre réseau :

1. Connectez un câble Ethernet au port LAN/PoE++ du AP.
2. Connectez l'autre extrémité du câble Ethernet à un port d'un commutateur connecté à votre réseau et à Internet.

   Si vous utilisez un commutateur PoE+, le port du commutateur connecté au APdoit pouvoir fournir une alimentation PoE+ de 30 W. Le AP nécessite une entrée 802.3at (PoE+).

   REMARQUE: Assurez-vous d'utiliser un switch 802.3at (PoE+) et non un switch 802.3af (PoE). Si le voyant reste orange cinq minutes après le démarrage duAP, il est possible que le APne reçoive pas une alimentation PoE suffisante. Pour plus d'informations, consultez la section Le AP fonctionne comme un PoE PD et le voyant clignote en vert en continu à la page 371.

   Lorsque le APdémarre ou est en train d'obtenir une adresse IP d'un serveur DHCP (ou d'un routeur fonctionnant en tant que serveur DHCP) sur votre réseau, le voyant clignote lentement en orange. Après environ trois minutes, le voyant devient bleu ou vert fixe et le AP est prêt à effectuer la configuration initiale.

Pour plus d'informations sur l'accès au AP pour la configuration initiale, reportez-vous à la section Connectez-vous au AP pour la configuration initiale à la page 29.

Connectez-vous au AP pour la configuration initiale

Après avoir configuré le AP, vous pouvez utiliser plusieurs méthodes pour vous y connecter pour la configuration initiale :

- Vous pouvez laisser le contrôleur NETGEAR engager à bord du AP. Pour plus d'informations, consultez la section Utilisez le contrôleur engage NETGEAR pour ajouter un point d'accès à un site engage à la page 30.
- Pour la gestion à distance de AP(et de plusieurs appareils et réseaux), vous pouvez utiliser le portail cloud Netgear insight sur un ordinateur ou une tablette ou l'application Netgear insight sur un appareil mobile iOS ou Android. Pour plus d'informations sur l'utilisation du portail cloud Insight ou de l'application Insight, consultez l'une des sections suivantes :
  - Connectez-vous sur Internet à l'aide du portail cloud Netgear insight à la page 32
  - Connectez-vous via WiFi à l'aide de l'application Netgear insight à la page 34
- Si vous utilisez APdans une configuration autonome, vous pouvez utiliser l'interface utilisateur du terminal sur un ordinateur ou une tablette. Pour plus d'informations sur l'utilisation de l'interface utilisateur du périphérique, reportez-vous à l'une des sections suivantes :
  - Connectez-vous via WiFi à l'interface utilisateur de l'appareil pour la configuration initiale à la page 37
  - Connectez-vous sur le LAN à l'interface utilisateur du périphérique pour la configuration initiale à la page 42
  - Configurez le AP hors ligne à l'aide d'un ordinateur directement connecté à la page 47

REMARQUE: Si votre réseau n'inclut pas de serveur DHCP (ou de routeur fonctionnant comme un serveur DHCP) et que vous n'effectuez pas la configuration initiale du système AP comme décrit dans l'une de ces sections, vous pouvez vous connecter uniquement au système AP et ne peut fournir une adresse IP qu'à cinq clients.AP Pour éviter cette situation, assurez-vous d'effectuer la configuration initiale du AP.

Utilisez le contrôleur engage NETGEAR pour ajouter un point d'accès à un site engage

Cette procédure décrit les étapes à suivre pour ajouter un AP à un site si APs'affiche dans le tableau périphériques découverts, c'est-à-dire APs'il s'agit d'un périphérique découvert. Si vous n'avez pas configuré le SSID global du site et défini la région et le comté pour le fonctionnement WiFi lors de la configuration initiale du AP, cette procédure décrit également ces étapes.

REMARQUE: Le AP doit exécuter la version 11,6 ou une version ultérieure du micrologiciel et doit être à l'état usine par défaut pour que le contrôleur d'engagement puisse l'intégrer.

Pour ajouter un AP à un site :

1. Sur votre ordinateur, dans le dossier dans lequel vous avez installé l'application de contrôleur, double-cliquez sur l'icône de l'application **engage** ou double-cliquez sur le raccourci **engage**.

   L'application s'ouvre et affiche une page de connexion.

2. Dans le champ **Login Name** (Nom de connexion), saisissez le nom d'utilisateur **admin**. Dans le champ **Password** (Mot de passe), saisissez le mot de passe du contrôleur que vous avez configuré lors de votre première connexion, puis cliquez sur le bouton **Login** (Connexion).

   La page Managed Devices (Appareils gérés) s'affiche.

3. **Si vous configurez plusieurs sites, dans le menu** Site, sélectionnez le site.

   La fenêtre contextuelle modifier la configuration réseau s'affiche.

   Effectuez l'une des opérations suivantes :

   - N'apportez aucune modification à la configuration réseau du site : Cliquez sur le bouton **Apply** (Appliquer).
   - Modifiez la configuration réseau du site : Modifiez la configuration réseau et cliquez sur le bouton **Apply** (Appliquer). Pour plus d'informations, consultez le Manuel de l'utilisateur du contrôleur Engage.

   La page périphériques gérés s'ajuste.

4. Dans le tableau périphériques découverts , cliquez sur le bouton **Onboard** du AP.

   Une fenêtre d'avertissement s'affiche.

5. Cliquez sur le bouton **Continue** (Continuer).

La fenêtre contextuelle Wireless Setup (Configuration sans fil) s'affiche.

6. Si vous n'avez pas encore configuré le SSID global du site, la région et le pays pour le fonctionnement du WiFi, configurez le paramètre suivant :

   a. Dans le champ **SSID**, saisissez le nom du réseau WiFi (SSID).

   b. Dans le champ **Password** (Mot de passe), saisissez le mot de passe d'accès au réseau WiFi, qui utilise la sécurité WPA-MPSK.

      Pour plus d'informations sur la sécurité WiFi, consultez le manuel de l'utilisateur du contrôleur Engage, que vous pouvez télécharger en visitant netgear.fr/support/download.

   c. Dans le menu **Region** (Région), sélectionnez la région du pays dans lequel se trouve le site par défaut. Après la configuration, vous ne pourrez pas modifier la région.

   d. Dans le menu **Country** (Pays), sélectionnez le pays dans lequel se trouve le site par défaut. Après la configuration, vous ne pourrez pas modifier le pays.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. La fenêtre contextuelle Add Device (Ajouter un appareil) s'ouvre.

   Étant donné que le point d'accès doit être défini sur ses paramètres par défaut, le bouton **Use device default password** (Utiliser le mot de passe par défaut de l'appareil) est automatiquement activé de sorte qu'il s'affiche en bleu ou en vert et se trouve à droite.

8. Cliquez sur le bouton **Single**.

   Les paramètres sont enregistrés.

   Le PA est déplacé vers le tableau des appareils gérés et le processus d'intégration est maintenant en cours.

   REMARQUE: À la fin de cette procédure, le contrôleur engage transmet le mot de passe du site au système AP (qui remplace le mot de passe par défaut). Si la version du micrologiciel du PA ne prend pas en charge le contrôleur, le contrôleur met automatiquement à jour le micrologiciel, après quoi l'appareil redémarre. Une fois ces processus terminés, le PA devient un appareil géré et passe de l'état en attente à l'état en ligne. L'opération peut prendre jusqu'à 10 minutes.

9. Pour enregistrer les paramètres dans la configuration en cours d'exécution, cliquez sur le bouton **Save** (Enregistrer) en haut à droite de la page.

Connectez-vous sur Internet à l'aide du portail cloud Netgear insight

Le portail Insight Cloud est disponible pour les titulaires d'un abonnement Insight Premium ou Insight Pro. Pour utiliser le portail cloud Netgear insight pour configurer et gérer AP, le AP doit déjà être connecté à Internet.

Pour plus d'informations sur le portail cloud Insight, consultez les pages suivantes :

- netgear.com/fr/business/services/insight
- kb.netgear.com/fr/000061848
- kb.netgear.com/fr/000044343

Votre compte NETGEAR est également votre compte Insight. Les identifiants de votre compte NETGEAR vous permettent de vous connecter en tant qu'utilisateur Insight Premium ou, si vous effectuez la mise à niveau vers un compte Insight Pro, en tant qu'utilisateur Insight Pro.

La figure suivante illustre le APconnecté à un commutateur PoE++, qui dispose d'une connexion redondante à un routeur réseau connecté à Internet. Les clients WiFi disposent de l'application Netgear insight installée ou ont accès au portail Cloud.

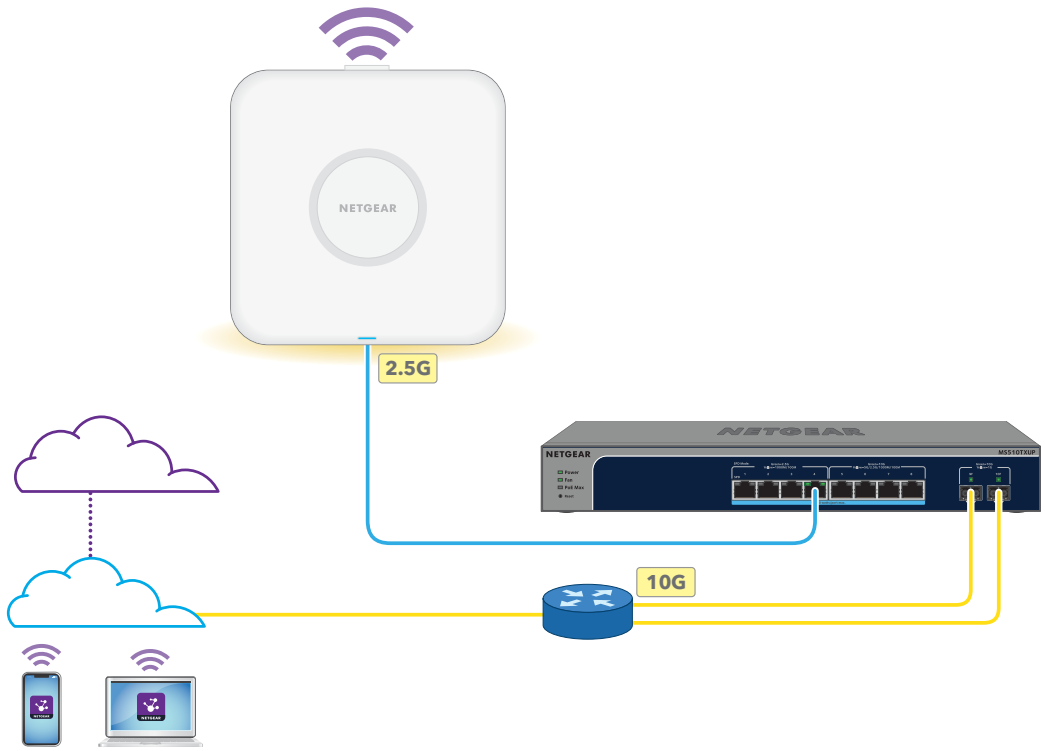

Illustration 5 : Configurez le AP dans une configuration Netgear insight

Pour vous connecter à APvia Internet via le portail cloud Insight :

1. Vérifiez que le PA est connecté à Internet.
2. Sur un ordinateur ou une tablette, consultez le site insight.netgear.com.

   La page de connexion au compte NETGEAR s'affiche.
3. Si vous n'avez pas encore de compte Insight, vous pouvez en créer un maintenant.

   Pour plus d'informations sur la création d'un compte Insight Premium ou pour effectuer la mise à niveau vers un compte Insight Pro, consultez l'article kb.netgear.com/000044343.
4. Saisissez l'adresse e-mail et le mot de passe de votre compte NETGEAR, puis appuyez sur le bouton **NETGEAR Sign In** (Connexion NETGEAR).
5. Si vous êtes un utilisateur Insight Pro uniquement, sélectionnez l'organisation à laquelle vous voulez ajouter le PA.
6. Ajoutez un emplacement réseau là où vous voulez ajouter le PA ou sélectionnez un emplacement réseau existant.
7. Cliquez sur le bouton **+ (Add Device)** (Ajouter un appareil).

   REMARQUE: Si vous utilisez Insight Pro, vous pouvez ajouter un appareil seul ou plusieurs appareils manageables via Insight en chargeant une liste des appareils en tant que fichier CSV.
8. Sur la page contextuelle Add New Device (Ajouter un nouvel appareil), saisissez le numéro de série du PA et l'adresse MAC, puis cliquez sur **Go** (Accéder).

   Le numéro de série et l'adresse MAC figurent sur l'APétiquette.
9. Dès qu'Insight a vérifié que le PA est un produit valide, vous pouvez, si vous le souhaitez, modifier le nom d'appareil du PA, puis cliquer sur **Next** (Suivant).

   Lorsque le PA a été ajouté avec succès au portail, une page affiche une confirmation que la configuration est en cours.

   REMARQUE: Si le PA est en ligne mais qu'Insight ne le détecte pas, le pare-feu de l'emplacement physique où est situé le PA peut empêcher la communication avec le cloud Insight. Dans cette situation, ajoutez les entrées de port et de DNS pour l'accès sortant au pare-feu. Pour en savoir plus, consultez l'article kb.netgear.com/000062467.

   Le PA se met à jour automatiquement avec la dernière version du firmware Insight et la configuration de l'emplacement Insight. Cela peut prendre jusqu'à 10 minutes, au cours desquelles le PA va redémarrer.

Le PA est à présent un appareil géré par Insight et connecté à la plateforme de gestion basée sur le cloud Insight. Si le voyant Power/Cloud (Alimentation/Cloud) était vert fixe, il s’allume en bleu fixe.

Vous pouvez utiliser le portail Insight Cloud ou l’application Insight pour configurer et gérer le PA.

REMARQUE: Si vous ajoutez APà un emplacement réseau Netgear insight et gérez APvia le portail cloud Insight ou l'application Insight, le mot de passe administrateur de APchange. En d'autres termes, après avoir ajouté APà un emplacement réseau Insight, le mot de passe réseau Insight de cet emplacement remplace le mot de passe admin. Pour accéder à l'interface utilisateur du périphérique, vous devez entrer le mot de passe réseau Insight et non le mot de passe admin. Si vous décidez par la suite de supprimer APde l'emplacement réseau Insight ou de passer en mode de gestion navigateur Web (voir Changez le mode de gestion en Netgear insight ou navigateur Web à la page 242), vous devez continuer à utiliser le mot de passe réseau Insight pour accéder à l'interface utilisateur du terminal jusqu'à ce que vous modifiiez manuellement le mot de passe admin sur AP.

Connectez-vous via WiFi à l'aide de l'application Netgear insight

L'application Netgear insight est disponible pour les abonnés Insight Premium et Insight Pro.

Vous pouvez installer l'application Netgear insight sur un appareil mobile iOS ou Android et configurer AP(et effectuer de nombreuses autres tâches).

Pour plus d'informations sur l'application Insight, consultez les pages suivantes :

- netgear.com/fr/business/services/insight
- kb.netgear.com/fr/000061848
- kb.netgear.com/fr/000044343

Votre compte NETGEAR est également votre compte Insight. Les identifiants de votre compte NETGEAR vous permettent de vous connecter en tant qu’utilisateur Insight Premium ou, si vous effectuez la mise à niveau vers un compte Insight Pro, en tant qu’utilisateur Insight Pro.

La figure suivante illustre le APconnecté à un commutateur PoE++, qui dispose d'une connexion redondante à un routeur réseau connecté à Internet. Les clients WiFi disposent de l'application Netgear insight installée ou ont accès au portail Cloud.

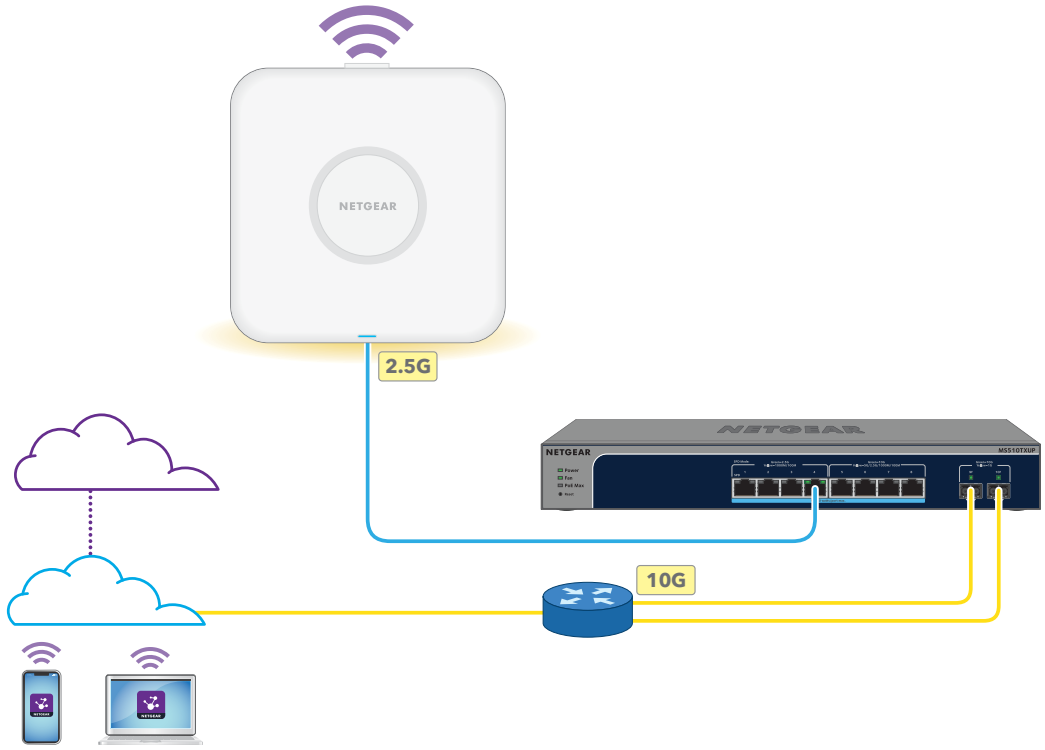

Illustration 6 : Configurez le AP dans une configuration Netgear insight

Pour vous connecter à APvia WiFi à l'aide d'un appareil mobile iOS ou Android :

1. Sur votre appareil mobile, rendez-vous dans la boutique d'applications, recherchez NETGEAR Insight et téléchargez la dernière version de l'application.

Download on the App Store

GET IT ON Google Play

NETGEAR

2. Sur votre appareil mobile, connectez-vous via WiFi au APréseau WiFi configuré de l' à l'aide de l'une des méthodes suivantes :

- **Scanner le code QR** : Scannez le code QR sur l'APétiquette située au bas du AP pour vous connecter au réseau WiFi configuré.
- **Se connecter manuellement** : le SSID de configuration figure sur l'étiquette du PA et est indiqué au format NETGEARxxxxxx-SETUP, où xxxxxx sont les six derniers chiffres de l'adresse MAC du PA. Le mot de passe par défaut est **sharedsecret**.

3. Lancez l'application Insight.
4. Si vous n’avez pas encore de compte Insight, vous pouvez en créer un maintenant.

   Pour plus d’informations sur la création d’un compte Insight Premium ou pour effectuer la mise à niveau vers un compte Insight Pro, consultez l’article kb.netgear.com/000044343.
5. Saisissez l'adresse électronique et le mot de passe de votre compte NETGEAR et appuyez sur **LOG IN** (Connexion).
6. Ajoutez un nouvel emplacement réseau là où vous voulez ajouter le PA en appuyant sur le bouton **Next** (Suivant), puis en appuyant sur OK**.**

   Vous pouvez également sélectionner un emplacement réseau existant.

   Le mot de passe de l'administrateur de l'appareil que vous avez saisi pour le nouvel emplacement réseau remplace le mot de passe existant de l'administrateur de l'appareil sur tous les appareils que vous avez ajoutés à l’emplacement réseau.

   Dans la plupart des situations, Insight détecte automatiquement le PA, ce qui peut prendre quelques minutes.
7. Pour ajouter le PA à votre emplacement réseau, effectuez l'une des opérations suivantes :
   - Si le PA est détecté automatiquement et répertorié dans la section Insight Manageable Devices (Appareils manageables par Insight), appuyez sur l'icône AP (PA), puis sur le bouton **ADD DEVICE** (AJOUTER UN APPAREIL).
   - Si le PA n'est pas détecté automatiquement ou si vous préférez utiliser une autre méthode pour ajouter le PA, appuyez sur l'icône **+** dans la barre supérieure, puis effectuez l'une des opérations suivantes :
     - Appuyez sur le bouton **NUMÉRISER LE CODE-BARRES OU LE code QR**, puis scannez APle code de l', qui se trouve sur APl'étiquette.
     - Appuyez sur le lien **entrer le numéro de série et l'adresse MAC**, puis saisissez manuellement APle numéro de série et l'adresse MAC du système, qui figurent sur APl'étiquette.
8. Le cas échéant, nommez le PA et appuyez sur le bouton **Next** (Suivant).

Le PA se met à jour automatiquement avec la dernière version du firmware Insight et la configuration de l'emplacement Insight. Cela peut prendre jusqu'à 10 minutes, au cours desquelles le PA va redémarrer.

Le PA est à présent un appareil géré par Insight et connecté à la plateforme de gestion basée sur le cloud Insight. Le voyant s'allume en bleu fixe dans ce mode.

Vous pouvez utiliser le portail Insight Cloud ou l’application Insight pour configurer et gérer le PA.

REMARQUE: Si vous ajoutez APà un emplacement réseau Netgear insight et gérez APvia le portail cloud Insight ou l'application Insight, le mot de passe administrateur de APchange. Autrement dit, le mot de passe réseau Insight pour cet emplacement remplace le mot de passe admin. Pour accéder à l'interface utilisateur du périphérique, vous devez entrer le mot de passe réseau Insight et non le mot de passe admin. Si vous décidez par la suite de supprimer APde l'emplacement réseau Insight ou de passer en mode de gestion navigateur Web (voir Changez le mode de gestion en Netgear insight ou navigateur Web à la page 242), vous devez continuer à utiliser le mot de passe réseau Insight pour accéder à l'interface utilisateur du terminal jusqu'à ce que vous modifiiez manuellement le mot de passe admin sur AP.

Connectez-vous via WiFi à l'interface utilisateur de l'appareil pour la configuration initiale

Cette section décrit comment se connecter pour la première fois au via WiFi à l'aide d'un ordinateur ou d'un périphérique mobile compatible WiFi (sans utiliser l'application Netgear insight) et comment APeffectuer la configuration initiale.

Pour vous connecter via WiFi à l'interface utilisateur de l'appareil pour la configuration initiale :

1. À partir de votre ordinateur ou appareil mobile, connectez-vous via WiFi au APréseau WiFi configuré de l' en utilisant l'une des méthodes suivantes :

- **Scanner le code QR** : Scannez le code QR sur l'APétiquette située au bas du AP pour vous connecter au réseau WiFi configuré.
- **Se connecter manuellement** : le SSID de configuration figure sur l'étiquette du PA et est indiqué au format NETGEARxxxxxx-SETUP, où xxxxxx sont les six derniers chiffres de l'adresse MAC du PA. Le mot de passe par défaut est **sharedsecret**.

2. Sur l'ordinateur ou le périphérique mobile, lancez un navigateur Web et, dans la barre d'adresse, tapez **http://aplogin.net**.

   REMARQUE: Vous ne pouvez utiliser **http://aplogin.net** que lors de la configuration initiale du AP.

   La page de connexion s'affiche.

   Il est possible que votre navigateur affiche un avertissement de sécurité en raison du certificat autosigné du PA, il s'agit d'un comportement attendu. Vous pouvez poursuivre ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez le APnom d'utilisateur et le mot de passe par défaut, puis cliquez sur le bouton **connexion**.

   Le nom d'utilisateur est **admin**. Le mot de passe par défaut est **password**. Le nom utilisateur et le mot de passe sont sensibles à la casse.

   La page de configuration aisée « Day Zero » s'affiche.

4. Sélectionnez le bouton radio **navigateur Web**.

   La page Day Zero Easy Setup s'ajuste pour afficher plusieurs options.

   REMARQUE: Une fois que vous avez enregistré les paramètres de base affichés sur la page, la page Day Zero Easy Setup ne s'affiche plus lorsque vous vous connectez. La page de connexion s'affiche à la place. Une fois connecté, le tableau de bord s'affiche.

5. Pour laisser le AP rechercher la dernière version du micrologiciel, cliquez sur le bouton **Rechercher une mise à niveau**.

   Si un nouveau micrologiciel est disponible pour le AP, nous vous recommandons de le mettre à niveau. Une fois la mise à niveau du micrologiciel terminée, APredémarre. Lorsque le AP est prêt, revenir à Étape 1 de cette procédure.

6. Spécifiez les paramètres comme décrit dans le tableau suivant.

Paramètre	Description
Pays / région	Dans le menu, sélectionnez le pays et la région dans lesquels fonctionne leAP. **Remarque** : Dans certains pays, le PA est vendu avec un paramètre Pays/Région préconfiguré et vous ne pouvez pas le modifier. **Remarque** : si votre pays ou région ne figure pas dans le menu, mettez à jour le micrologiciel du PA, puis revérifiez. Si votre pays ou votre région ne figure toujours pas dans la liste, contactez l'assistance NETGEAR. **Remarque** : vérifiez que le pays est défini sur l'emplacement où l'appareil est installé. L'utilisation du routeur dans une région autre que celle indiquée ici peut être interdite par la loi. Vous êtes responsable de la conformité aux réglementations locales, régionales et nationales définies pour les canaux, les niveaux de puissance et les plages de fréquences.
Fuseau horaire	Dans le menu, sélectionnez le fuseau horaire du pays et de la région dans lesquels fonctionne leAP.
Client DHCP	Par défaut, le client DHCP du système AP permet au système de APrecevoir une adresse IP d'un serveur DHCP (ou d'un routeur fonctionnant comme un serveur DHCP) de votre réseau. Pour configurer le AP avec une adresse IP statique (fixe), procédez comme suit : a. Sélectionnez le bouton radio **désactiver**. Des champs supplémentaires s'affichent. b. Spécifiez l'adresse IP, le masque de sous-réseau IP, l'adresse IP de la passerelle par défaut et l'adresse IP du serveur DNS.
Nom du AP	Vous pouvez également saisir un nouveau nom pour le AP. Le nom doit contenir des caractères alphanumériques, au moins un caractère alphabétique, ne peut pas dépasser 64 caractères et peut contenir des tirets mais ne peut pas commencer ou se terminer par un tiret. Par défaut, le AP nom est Netgear xxxxxx, xxxxxx représentant les six derniers chiffres hexadécimaux de APl'adresse MAC du système.
Nouveau mot de passe de connexion AP	Saisissez un nouveau mot de passe administrateur. Il s'agit du mot de passe que vous devez utiliser pour vous connecter à l'APinterface utilisateur du terminal de . (Il *ne* s'agit *pas* du mot de passe que vous utilisez pour accéder au WiFi.) Le mot de passe doit comporter entre 8 et 64 caractères et contenir au moins une lettre majuscule, une lettre minuscule et un chiffre. Enregistrez le mot de passe pour une utilisation ultérieure.
Confirmation du nouveau mot de passe	Saisissez exactement le même mot de passe que celui que vous avez saisi dans le champ **Nouveau mot de passe de connexion AP**.
SSID	Vous ne pouvez pas utiliser le SSID de configuration pour un fonctionnement normal. Le SSID de configuration est réservé à la configuration initiale. Saisissez un nouveau nom de 32 caractères maximum. Vous pouvez utiliser une combinaison de caractères alphanumériques et spéciaux, à l'exception des guillemets (") et d'une barre oblique inverse (\).

7. Dans le menu **authentification**, sélectionnez l'un des types d'authentification suivants pour le réseau WiFi et, le cas échéant, définissez une nouvelle phrase de passe (clé réseau ou mot de passe WiFi) pour le réseau WiFi :

- **Ouvrir**. Réseau WiFi ouvert qui n'offre aucune sécurité. Tout périphérique WiFi peut se connecter au réseau WiFi. Nous vous recommandons *de ne pas* utiliser un réseau WiFi ouvert existant mais de configurer la sécurité WiFi. Cependant, un réseau ouvert hérité peut être approprié pour un hotspot WiFi.

  REMARQUE: Il n'est pas nécessaire de créer une phrase de passe pour un réseau ouvert.

  Si vous sélectionnez **ouvrir** dans le menu **authentification**, la case à cocher **ouverture avancée** s'affiche.

  - **Case à cocher ouverture améliorée désactivée**: Le réseau WiFi est un réseau ouvert hérité sans aucune sécurité. Il s'agit de l'option par défaut pour un réseau ouvert. Les clients ne sont pas authentifiés, le trafic n'est pas chiffré et la norme 802.11w (PMF) est automatiquement désactivée.
  - **Case à cocher ouvrir améliorée sélectionnée**: La fonction d'ouverture Wi-Fi améliorée est activée. Cette fonctionnalité est basée sur le chiffrement sans fil opportuniste (OWE). Le cryptage est défini sur CCM mode Protocol (CCMP) et 802.11w (PMF) est automatiquement défini sur obligatoire. Si vous cochez la case **ouverture améliorée**, la case **autoriser les périphériques à se connecter avec ouverture** s'affiche.

    Si vous cochez la case **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi peut accepter les clients qui prennent en charge la fonction d'ouverture améliorée WiFi et les clients qui ne le prennent pas en charge. Pour les clients qui ne prennent pas en charge la fonction Wi-Fi Open Enhanced, le trafic n'est pas crypté.

    Si vous désactivez la case à cocher **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi ne peut accepter que les clients qui prennent en charge la fonction d'ouverture améliorée WiFi.
- **WPA2 personnel**: Cette option permet uniquement aux clients WiFi qui prennent en charge WPA2 de se connecter au SSID. Sélectionnez cette option si tous les clients WiFi prennent en charge WPA2. Cette option utilise le cryptage AES.
- **WPA2/WPA personnel**: Cette option permet aux clients Wifi WPA et WPA2 de se connecter au SSID. Cette option utilise le cryptage TKIP et AES. Les paquets de diffusion utilisent TKIP. Pour les transmissions unicast (c'est-à-dire point à point), les clients WPA utilisent TKIP et les clients WPA2 utilisent AES.

- **WPA3 personnel**: Cette option permet uniquement aux clients WiFi qui prennent en charge WPA3 de se connecter au SSID. Sélectionnez cette option si tous les clients WiFi prennent en charge WPA3. Cette option utilise le cryptage SAE.
- **WPA3/WPA2 personnel**: Cette option permet aux clients Wifi WPA2 et WPA3 de se connecter au SSID. Cette option utilise le cryptage AES et SAE. Les clients WPA2 utilisent AES et les clients WPA3 utilisent SAE.

Remarque : Une fois le processus de configuration terminé, vous pouvez configurer la sécurité WPA2 entreprise ou WPA3 entreprise avec des serveurs RADIUS. Pour plus d'informations, consultez la section Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90.

8. Dans le champ **phrase de passe**, saisissez une nouvelle phrase de passe pour le réseau WiFi.

   REMARQUE: Par défaut, la case **phrase de passe complexe** est cochée pour appliquer les exigences minimales de mot de passe qui contribuent à améliorer la sécurité du réseau sans fil. Pour désactiver la fonction phrase de passe complexe :

   - Cochez la case **phrase de passe complexe**.
   - Une fenêtre contextuelle de confirmation s'affiche.
   - Cliquez sur le bouton **OK** (Enregistrer).

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Une fenêtre contextuelle affiche l'adresse IP, le nouveau réseau WiFi et le mot de passe (phrase de passe).

   Si vous avez spécifié une adresse IP statique, enregistrez les informations d'adresse IP car vous devez saisir l'adresse IP lorsque vous vous reconnectez.

   Vous êtes déconnecté du AP. Si vous avez modifié le pays par défaut, le AP redémarre.

10. Reconnectez-vous via WiFi au APréseau WiFi du à l'aide du nouveau SSID et de la nouvelle phrase de passe que vous venez de définir sur la page Day Zero Easy Setup.
11. Saisissez l'APadresse IP dans la barre d'adresse du navigateur.

    Si vous avez modifié l'adresse IP, saisissez l'adresse IP que vous avez spécifiée dans Étape 6.

    Il est possible que votre navigateur affiche un avertissement de sécurité en raison du certificat autosigné du PA, il s'agit d'un comportement attendu. Vous pouvez poursuivre ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

La page de connexion s'affiche.

12. Saisissez le APnom d'utilisateur et le mot de passe, puis cliquez sur le bouton **connexion**.

    Le nom d'utilisateur est **admin**. Le mot de passe est celui que vous venez de définir sur la page Day Zero Easy Setup. Le nom utilisateur et le mot de passe sont sensibles à la casse.

    Le tableau de bord s'affiche. Vous pouvez désormais personnaliser APles paramètres de votre environnement réseau.

Connectez-vous sur le LAN à l'interface utilisateur du périphérique pour la configuration initiale

La procédure suivante suppose que votre réseau comprend un serveur DHCP (ou routeur fonctionnant comme un serveur DHCP) et que le AP et votre ordinateur se trouvent sur le même réseau local. Par défaut, le switch fonctionne comme un client DHCP.

Pour vous connecter via le LAN à l'interface utilisateur du périphérique pour la configuration initiale :

1. Pour déterminer l'adresse IP attribuée par le serveur DHCP au AP, accédez au serveur DHCP ou utilisez un scanner de réseau IP.

   Si vous utilisez un ordinateur Windows, lancez l'Explorateur de fichiers (ou l'Explorateur Windows), sélectionnez **réseau** dans le volet de navigation, cliquez avec le bouton droit de la souris sur l'APicône du périphérique et sélectionnez **Propriétés** pour afficher l'adresse IP.

   REMARQUE: Vous pouvez également utiliser l'application Netgear insight pour découvrir l'adresse IP attribuée au AP. Pour plus d'informations, consultez la section Connectez-vous via WiFi à l'aide de l'application Netgear insight à la page 34.

2. Sur l'ordinateur, lancez un navigateur Web et, dans la barre d'adresse, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Il est possible que votre navigateur affiche un avertissement de sécurité en raison du certificat autosigné du PA, il s'agit d'un comportement attendu. Vous pouvez poursuivre ou ajouter une exception pour l'avertissement de sécurité. Pour plus

d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez le APnom d'utilisateur et le mot de passe par défaut, puis cliquez sur le bouton **connexion**.

   Le nom d'utilisateur est **admin**. Le mot de passe par défaut est **password**. Le nom utilisateur et le mot de passe sont sensibles à la casse.

   La page de configuration aisée « Day Zero » s'affiche.

4. Sélectionnez le bouton radio **navigateur Web**.

   La page Day Zero Easy Setup s'ajuste pour afficher plusieurs options.

   REMARQUE: Une fois que vous avez enregistré les paramètres de base affichés sur la page, la page Day Zero Easy Setup ne s'affiche plus lorsque vous vous connectez. La page de connexion s'affiche à la place. Une fois connecté, le tableau de bord s'affiche.

5. Pour laisser le AP rechercher la dernière version du micrologiciel, cliquez sur le bouton **Rechercher une mise à niveau**.

   Si un nouveau micrologiciel est disponible pour le AP, nous vous recommandons de le mettre à niveau. Une fois la mise à niveau du micrologiciel terminée, APredémarre. Lorsque le AP est prêt, en fonction de votre situation, revenez à Étape 2 ou Étape 3 de cette procédure.

6. Spécifiez les paramètres comme décrit dans le tableau suivant.

Paramètre	Description
Pays / région	Dans le menu, sélectionnez le pays et la région dans lesquels fonctionne leAP. **Remarque** : Dans certains pays, le PA est vendu avec un paramètre Pays/Région préconfiguré et vous ne pouvez pas le modifier. **Remarque** : si votre pays ou région ne figure pas dans le menu, mettez à jour le micrologiciel du PA, puis revérifiez. Si votre pays ou votre région ne figure toujours pas dans la liste, contactez l'assistance NETGEAR. **Remarque** : vérifiez que le pays est défini sur l'emplacement où l'appareil est installé. L'utilisation du routeur dans une région autre que celle indiquée ici peut être interdite par la loi. Vous êtes responsable de la conformité aux réglementations locales, régionales et nationales définies pour les canaux, les niveaux de puissance et les plages de fréquences.
Fuseau horaire	Dans le menu, sélectionnez le fuseau horaire du pays et de la région dans lesquels fonctionne leAP.

(A continué)

Paramètre	Description
Client DHCP	Par défaut, le client DHCP du système AP permet au système de APrecevoir une adresse IP d'un serveur DHCP (ou d'un routeur fonctionnant comme un serveur DHCP) de votre réseau. Pour configurer le AP avec une adresse IP statique (fixe), procédez comme suit : a. Sélectionnez le bouton radio **désactiver**. Des champs supplémentaires s'affichent. b. Spécifiez l'adresse IP, le masque de sous-réseau IP, l'adresse IP de la passerelle par défaut et l'adresse IP du serveur DNS.
Nom du AP	Vous pouvez également saisir un nouveau nom pour le AP. Le nom doit contenir des caractères alphanumériques, au moins un caractère alphabétique, ne peut pas dépasser 64 caractères et peut contenir des tirets mais ne peut pas commencer ou se terminer par un tiret. Par défaut, le AP nom est Netgear xxxxxx, xxxxxx représentant les six derniers chiffres hexadécimaux de APl'adresse MAC du système.
Nouveau mot de passe de connexion AP	Saisissez un nouveau mot de passe administrateur. Il s'agit du mot de passe que vous devez utiliser pour vous connecter à l'APinterface utilisateur du terminal de . (Il *ne* s'agit *pas* du mot de passe que vous utilisez pour accéder au WiFi.) Le mot de passe doit comporter entre 8 et 64 caractères et contenir au moins une lettre majuscule, une lettre minuscule et un chiffre. Enregistrez le mot de passe pour une utilisation ultérieure.
Confirmation du nouveau mot de passe	Saisissez exactement le même mot de passe que celui que vous avez saisi dans le champ **Nouveau mot de passe de connexion AP**.
SSID	Vous ne pouvez pas utiliser le SSID de configuration pour un fonctionnement normal. Le SSID de configuration est réservé à la configuration initiale. Saisissez un nouveau nom de 32 caractères maximum. Vous pouvez utiliser une combinaison de caractères alphanumériques et spéciaux, à l'exception des guillemets (") et d'une barre oblique inverse (\).

7. Dans le menu **authentification**, sélectionnez l'un des types d'authentification suivants pour le réseau WiFi et, le cas échéant, définissez une nouvelle phrase de passe (clé réseau ou mot de passe WiFi) pour le réseau WiFi :

   - **Ouvrir**. Réseau WiFi ouvert qui n'offre aucune sécurité. Tout périphérique WiFi peut se connecter au réseau WiFi. Nous vous recommandons *de ne pas* utiliser un réseau WiFi ouvert existant mais de configurer la sécurité WiFi. Cependant, un réseau ouvert hérité peut être approprié pour un hotspot WiFi.

     REMARQUE: Il n'est pas nécessaire de créer une phrase de passe pour un réseau ouvert.

Si vous sélectionnez **ouvrir** dans le menu **authentification**, la case à cocher **ouverture avancée** s'affiche.

- **Case à cocher ouverture améliorée désactivée**: Le réseau WiFi est un réseau ouvert hérité sans aucune sécurité. Il s'agit de l'option par défaut pour un réseau ouvert. Les clients ne sont pas authentifiés, le trafic n'est pas chiffré et la norme 802.11w (PMF) est automatiquement désactivée.
- **Case à cocher ouvrir améliorée sélectionnée**: La fonction d'ouverture Wi-Fi améliorée est activée. Cette fonctionnalité est basée sur le chiffrement sans fil opportuniste (OWE). Le cryptage est défini sur CCM mode Protocol (CCMP) et 802.11w (PMF) est automatiquement défini sur obligatoire. Si vous cochez la case **ouverture améliorée**, la case **autoriser les périphériques à se connecter avec ouverture** s'affiche.

  Si vous cochez la case **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi peut accepter les clients qui prennent en charge la fonction d'ouverture améliorée WiFi et les clients qui ne le prennent pas en charge. Pour les clients qui ne prennent pas en charge la fonction Wi-Fi Open Enhanced, le trafic n'est pas crypté.

  Si vous désactivez la case à cocher **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi ne peut accepter que les clients qui prennent en charge la fonction d'ouverture améliorée WiFi.

- **WPA2 personnel**: Cette option permet uniquement aux clients WiFi qui prennent en charge WPA2 de se connecter au SSID. Sélectionnez cette option si tous les clients WiFi prennent en charge WPA2. Cette option utilise le cryptage AES.
- **WPA2/WPA personnel**: Cette option permet aux clients Wifi WPA et WPA2 de se connecter au SSID. Cette option utilise le cryptage TKIP et AES. Les paquets de diffusion utilisent TKIP. Pour les transmissions unicast (c'est-à-dire point à point), les clients WPA utilisent TKIP et les clients WPA2 utilisent AES.
- **WPA3 personnel**: Cette option permet uniquement aux clients WiFi qui prennent en charge WPA3 de se connecter au SSID. Sélectionnez cette option si tous les clients WiFi prennent en charge WPA3. Cette option utilise le cryptage SAE.
- **WPA3/WPA2 personnel**: Cette option permet aux clients Wifi WPA2 et WPA3 de se connecter au SSID. Cette option utilise le cryptage AES et SAE. Les clients WPA2 utilisent AES et les clients WPA3 utilisent SAE.

Remarque : Une fois le processus de configuration terminé, vous pouvez configurer la sécurité WPA2 entreprise ou WPA3 entreprise avec des serveurs RADIUS. Pour

plus d'informations, consultez la section Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90.

8. Dans le champ **phrase de passe**, saisissez une nouvelle phrase de passe pour le réseau WiFi.

   REMARQUE: Par défaut, la case **phrase de passe complexe** est cochée pour appliquer les exigences minimales de mot de passe qui contribuent à améliorer la sécurité du réseau sans fil. Pour désactiver la fonction phrase de passe complexe :

   - Cochez la case **phrase de passe complexe**.
   - Une fenêtre contextuelle de confirmation s'affiche.
   - Cliquez sur le bouton **OK** (Enregistrer).

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Une fenêtre contextuelle affiche l'adresse IP, le nouveau réseau WiFi et le mot de passe (phrase de passe).

   Si vous avez spécifié une adresse IP statique, enregistrez les informations d'adresse IP car vous devez saisir l'adresse IP lorsque vous vous reconnectez.

   Si vous avez modifié le pays par défaut, le AP redémarre.

   REMARQUE: Ne fermez pas la page !

   Au bout d'une courte période, le tableau de bord s'affiche automatiquement. Si le tableau de bord ne s'affiche pas, par exemple parce que vous avez attribué une adresse IP statique, passez à l'étape suivante.

   Vous pouvez désormais personnaliser APles paramètres de votre environnement réseau.

10. Si le tableau de bord ne s'affiche pas automatiquement, procédez comme suit :
    a. Effectuez l'une des actions suivantes :
       - Si vous avez attribué une adresse IP statique au AP, saisissez l'adresse IP que vous avez spécifiée dans la Étape 6barre d'adresse du navigateur Web.
       - Si vous n'avez pas attribué d'adresse IP statique, saisissez à nouveau l'adresse IP affichée dans la barre d'adresse du navigateur Web. Si cela ne fonctionne pas, notez l'adresse IP, fermez le navigateur Web, relancez-le, puis saisissez l'adresse IP dans la barre d'adresse du navigateur Web.
       - Si vous n'avez pas attribué d'adresse IP statique et que vous avez fermé la page de sorte que vous ne puissiez pas voir l'adresse IP du AP, utilisez un analyseur IP, un outil de découverte de réseau ou accédez au serveur DHCP pour découvrir l'adresse IP du APdans votre réseau.

REMARQUE: Vous pouvez également utiliser l'application Netgear insight pour découvrir l'adresse IP attribuée au AP. Pour plus d'informations, consultez la section Connectez-vous via WiFi à l'aide de l'application Netgear insight à la page 34.

Ensuite, lancez un navigateur et tapez l'adresse IP dans la barre d'adresse.

Il est possible que votre navigateur affiche un avertissement de sécurité en raison du certificat autosigné du PA, il s'agit d'un comportement attendu. Vous pouvez poursuivre ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

La page de connexion s'affiche.

b. Saisissez le APnom d'utilisateur et le mot de passe, puis cliquez sur le bouton **connexion**.

Le nom d'utilisateur est **admin**. Le mot de passe est celui que vous venez de définir sur la page Day Zero Easy Setup. Le nom utilisateur et le mot de passe sont sensibles à la casse.

Le tableau de bord s'affiche. Vous pouvez désormais personnaliser APles paramètres de votre environnement réseau.

Configurez le AP hors ligne à l'aide d'un ordinateur directement connecté

Vous pouvez mettre le AP hors ligne (c'est-à-dire le déconnecter de votre réseau), connecter un ordinateur via un câble Ethernet au port LAN du APet vous connecter au APvia son adresse IP par défaut afin de pouvoir le configurer hors ligne. Une fois la configuration terminée, vous pouvez mettre le AP en ligne.

REMARQUE: Comme le AP n'est pas connecté à un commutateur PoE++, vous pouvez utiliser cette méthode de configuration uniquement si vous disposez d'un adaptateur secteur pour le AP.

Pour se connecter au APà l'aide d'un ordinateur directement connecté au port LAN du AP:

1. Enregistrez l'adresse IP et le masque de sous-réseau de votre ordinateur afin de pouvoir rétablir ces paramètres ultérieurement.
2. Changez temporairement l'adresse IP de votre ordinateur en 192.168.0.210 avec 255.255.255.0 comme masque de sous-réseau.

(Vous pouvez en fait utiliser n'importe quelle adresse IP comprise entre 192.168.0,2 et 192.168.0.254, à l'exception de l'adresse IP 192.168.0,100, qui est l'adresse IP par défaut du AP.)

Pour plus d'informations sur la modification de l'adresse IP sur votre ordinateur, consultez l'aide ou la documentation de votre ordinateur.

3. Utilisez le câble Ethernet pour connecter votre ordinateur à un port de réseau local Ethernet du routeur.
4. Sur l'ordinateur, lancez un navigateur Web et tapez **192.168.0.100** dans la barre d'adresse.

   La page de connexion s'affiche.

   Il est possible que votre navigateur affiche un avertissement de sécurité en raison du certificat autosigné du PA, il s'agit d'un comportement attendu. Vous pouvez poursuivre ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
5. Saisissez le APnom d'utilisateur et le mot de passe par défaut, puis cliquez sur le bouton **connexion**.

   Le nom d'utilisateur est **admin**. Le mot de passe par défaut est **password**. Le nom utilisateur et le mot de passe sont sensibles à la casse.

   La page de configuration aisée « Day Zero » s'affiche.
6. Sélectionnez le bouton radio **navigateur Web**.

   La page Day Zero Easy Setup s'ajuste pour afficher plusieurs options.

   REMARQUE: Une fois que vous avez enregistré les paramètres de base affichés sur la page, la page Day Zero Easy Setup ne s'affiche plus lorsque vous vous connectez. Une fenêtre de connexion s'affiche à la place. Une fois connecté, le tableau de bord s'affiche.
7. Pour laisser le AP rechercher la dernière version du micrologiciel, cliquez sur le bouton **Rechercher une mise à niveau**.

   Si un nouveau micrologiciel est disponible pour le AP, nous vous recommandons de le mettre à niveau. Une fois la mise à niveau du micrologiciel terminée, APredémarre. Lorsque le AP est prêt, en fonction de votre situation, revenez à Étape 4 ou Étape 5 de cette procédure.
8. Spécifiez les paramètres comme décrit dans le tableau suivant.

Paramètre	Description
Pays / région	Dans le menu, sélectionnez le pays et la région dans lesquels fonctionne leAP. **Remarque** : Dans certains pays, le PA est vendu avec un paramètre Pays/Région préconfiguré et vous ne pouvez pas le modifier. **Remarque** : si votre pays ou région ne figure pas dans le menu, mettez à jour le micrologiciel du PA, puis revérifiez. Si votre pays ou votre région ne figure toujours pas dans la liste, contactez l'assistance NETGEAR. **Remarque** : vérifiez que le pays est défini sur l'emplacement où l'appareil est installé. L'utilisation du routeur dans une région autre que celle indiquée ici peut être interdite par la loi. Vous êtes responsable de la conformité aux réglementations locales, régionales et nationales définies pour les canaux, les niveaux de puissance et les plages de fréquences.
Fuseau horaire	Dans le menu, sélectionnez le fuseau horaire du pays et de la région dans lesquels fonctionne leAP.
Client DHCP	Par défaut, le client DHCP du système AP permet au système de APrecevoir une adresse IP d'un serveur DHCP (ou d'un routeur fonctionnant comme un serveur DHCP) de votre réseau. Pour configurer le AP avec une adresse IP statique (fixe), procédez comme suit : a. Sélectionnez le bouton radio **désactiver**. Des champs supplémentaires s'affichent. b. Spécifiez l'adresse IP, le masque de sous-réseau IP, l'adresse IP de la passerelle par défaut et l'adresse IP du serveur DNS.
Nom du AP	Vous pouvez également saisir un nouveau nom pour le AP. Le nom doit contenir des caractères alphanumériques, au moins un caractère alphabétique, ne peut pas dépasser 64 caractères et peut contenir des tirets mais ne peut pas commencer ou se terminer par un tiret. Par défaut, le AP nom est Netgear xxxxxx, xxxxxx représentant les six derniers chiffres hexadécimaux de APl'adresse MAC du système.
Nouveau mot de passe de connexion AP	Saisissez un nouveau mot de passe administrateur. Il s'agit du mot de passe que vous devez utiliser pour vous connecter à l'APinterface utilisateur du terminal de . (Il *ne* s'agit *pas* du mot de passe que vous utilisez pour accéder au WiFi.) Le mot de passe doit comporter entre 8 et 64 caractères et contenir au moins une lettre majuscule, une lettre minuscule et un chiffre. Enregistrez le mot de passe pour une utilisation ultérieure.
Confirmation du nouveau mot de passe	Saisissez exactement le même mot de passe que celui que vous avez saisi dans le champ **Nouveau mot de passe de connexion AP**.
SSID	Vous ne pouvez pas utiliser le SSID de configuration pour un fonctionnement normal. Le SSID de configuration est réservé à la configuration initiale. Saisissez un nouveau nom de 32 caractères maximum. Vous pouvez utiliser une combinaison de caractères alphanumériques et spéciaux, à l'exception des guillemets (") et d'une barre oblique inverse (\).

9. Dans le menu **authentification**, sélectionnez l'un des types d'authentification suivants pour le réseau WiFi et, le cas échéant, définissez une nouvelle phrase de passe (clé réseau ou mot de passe WiFi) pour le réseau WiFi :

- **Ouvrir**. Réseau WiFi ouvert qui n'offre aucune sécurité. Tout périphérique WiFi peut se connecter au réseau WiFi. Nous vous recommandons *de ne pas* utiliser un réseau WiFi ouvert existant mais de configurer la sécurité WiFi. Cependant, un réseau ouvert hérité peut être approprié pour un hotspot WiFi.

  REMARQUE: Il n'est pas nécessaire de créer une phrase de passe pour un réseau ouvert.

  Si vous sélectionnez **ouvrir** dans le menu **authentification**, la case à cocher **ouverture avancée** s'affiche.

  - **Case à cocher ouverture améliorée désactivée**: Le réseau WiFi est un réseau ouvert hérité sans aucune sécurité. Il s'agit de l'option par défaut pour un réseau ouvert. Les clients ne sont pas authentifiés, le trafic n'est pas chiffré et la norme 802.11w (PMF) est automatiquement désactivée.
  - **Case à cocher ouvrir améliorée sélectionnée**: La fonction d'ouverture Wi-Fi améliorée est activée. Cette fonctionnalité est basée sur le chiffrement sans fil opportuniste (OWE). Le cryptage est défini sur CCM mode Protocol (CCMP) et 802.11w (PMF) est automatiquement défini sur obligatoire. Si vous cochez la case **ouverture améliorée**, la case **autoriser les périphériques à se connecter avec ouverture** s'affiche.

    Si vous cochez la case **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi peut accepter les clients qui prennent en charge la fonction d'ouverture améliorée WiFi et les clients qui ne le prennent pas en charge. Pour les clients qui ne prennent pas en charge la fonction Wi-Fi Open Enhanced, le trafic n'est pas crypté.

    Si vous désactivez la case à cocher **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi ne peut accepter que les clients qui prennent en charge la fonction d'ouverture améliorée WiFi.
- **WPA2 personnel**: Cette option permet uniquement aux clients WiFi qui prennent en charge WPA2 de se connecter au SSID. Sélectionnez cette option si tous les clients WiFi prennent en charge WPA2. Cette option utilise le cryptage AES.
- **WPA2/WPA personnel**: Cette option permet aux clients Wifi WPA et WPA2 de se connecter au SSID. Cette option utilise le cryptage TKIP et AES. Les paquets de diffusion utilisent TKIP. Pour les transmissions unicast (c'est-à-dire point à point), les clients WPA utilisent TKIP et les clients WPA2 utilisent AES.

- **WPA3 personnel**: Cette option permet uniquement aux clients WiFi qui prennent en charge WPA3 de se connecter au SSID. Sélectionnez cette option si tous les clients WiFi prennent en charge WPA3. Cette option utilise le cryptage SAE.
- **WPA3/WPA2 personnel**: Cette option permet aux clients Wifi WPA2 et WPA3 de se connecter au SSID. Cette option utilise le cryptage AES et SAE. Les clients WPA2 utilisent AES et les clients WPA3 utilisent SAE.

Remarque : Une fois le processus de configuration terminé, vous pouvez configurer la sécurité WPA2 entreprise ou WPA3 entreprise avec des serveurs RADIUS. Pour plus d'informations, consultez la section Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90.

10. Dans le champ **phrase de passe**, saisissez une nouvelle phrase de passe pour le réseau WiFi.

    REMARQUE: Par défaut, la case **phrase de passe complexe** est cochée pour appliquer les exigences minimales de mot de passe qui contribuent à améliorer la sécurité du réseau sans fil. Pour désactiver la fonction phrase de passe complexe :

    - Cochez la case **phrase de passe complexe**.
    - Une fenêtre contextuelle de confirmation s'affiche.
    - Cliquez sur le bouton **OK** (Enregistrer).

11. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés. Une fenêtre contextuelle affiche l'adresse IP, le nouveau réseau WiFi et le mot de passe (phrase de passe).

    Si vous avez spécifié une adresse IP statique, enregistrez les informations d'adresse IP car vous devez saisir l'adresse IP lorsque vous vous reconnectez.

    Vous êtes déconnecté du AP. Si vous avez modifié le pays par défaut, le AP redémarre.

12. Après quelques minutes, si la fenêtre de connexion ne s'affiche pas automatiquement, tapez **192.168.0.100** dans la barre d'adresse de votre navigateur.

    Si vous avez modifié l'adresse IP, saisissez l'adresse IP que vous avez enregistrée dans Étape 8.

    Il est possible que votre navigateur affiche un avertissement de sécurité en raison du certificat autosigné du PA, il s'agit d'un comportement attendu. Vous pouvez poursuivre ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

    La page de connexion s'affiche.

13. Saisissez le APnom d'utilisateur et le mot de passe, puis cliquez sur le bouton **connexion**.

    Le nom d'utilisateur est **admin**. Le mot de passe est celui que vous venez de définir sur la page Day Zero Easy Setup. Le nom utilisateur et le mot de passe sont sensibles à la casse.

    Le tableau de bord s’affiche. Vous pouvez désormais personnaliser APles paramètres de votre environnement réseau.

14. Après avoir terminé le processus de configuration, ou les deux, vous pouvez rétablir les paramètres d'adresse IP d'origine de l'ordinateur.

Connectez-vous au AP après la configuration initiale

Après la configuration initiale, le AP est prêt à être utilisé et vous pouvez modifier les paramètres et surveiller le trafic.

Pour vous connecter à l'APinterface utilisateur du terminal de :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

Sur cette page figurent plusieurs volets qui vous permettent de voir le statut de votre PR460X d'un seul coup d'œil.

Pour plus d'informations sur le tableau de bord et ses différents volets, reportez-vous à la section Surveillez le AP et le réseau à la page 284.

Informations d'identification de l'interface utilisateur du périphérique

Les informations de cette section s'appliquent à l'accès à l'interface utilisateur du périphérique. La manière dont vous accédez à l'interface utilisateur du terminal dépend de si vous intégrez le AP à une application de gestion telle que le contrôleur NETGEAR engage ou Netgear insight.

REMARQUE: NETGEAR Insight et le contrôleur Engage sont des méthodes de gestion mutuellement exclusives.

Pour accéder à l'interface utilisateur du périphérique, utilisez l'une des informations d'identification suivantes :

- **Vous intégrez le point d'accès au contrôleur NETGEAR engage : Utilisez le mot de passe du site engage** .

Une fois que vous avez intégré le switch à un site Engage, le mot de passe de ce dernier remplace le mot de passe administrateur du switch pour l'interface utilisateur de l'appareil. Pour accéder à l'interface utilisateur de l'appareil, vous devez saisir le mot de passe du site Engage.

REMARQUE: Lorsque le contrôleur d'engagement gère AP, les paramètres des fonctions que vous pouvez gérer via le contrôleur d'engagement sont masqués dans l'interface utilisateur du périphérique. Cependant, à l'aide de l'interface utilisateur du périphérique, vous pouvez toujours gérer les paramètres de certaines fonctionnalités. En outre, les tâches de surveillance, de maintenance et de diagnostic restent disponibles dans l'interface utilisateur du périphérique.

- **Vous utilisez uniquement l'interface utilisateur du périphérique : Utilisez le mot de passe administrateur AP** .

  Vous pouvez accéder à l'interface utilisateur du terminal à l'aide de votre mot de passe administrateur.

  La première fois que vous accédez à l'interface utilisateur du périphérique, entrez le mot de passe administrateur par défaut (password), après quoi vous devez personnaliser le mot de passe pour plus de sécurité. Chaque fois que vous vous connectez à l'interface utilisateur du terminal, utilisez votre mot de passe administrateur personnalisé.

- **Vous ajoutez le point d'accès à un emplacement réseau Netgear insight : Utilisez le mot de passe d'emplacement réseau Insight** .

  Si vous conservez le mode Insight activé dans l'interface utilisateur du terminal (paramètre par défaut), *après* avoir ajouté APà un emplacement réseau Insight, le mot de passe de l'emplacement réseau Insight remplace le APmot de passe administrateur de l'interface utilisateur du terminal. Pour accéder à l'interface utilisateur de l'appareil, vous devez saisir le mot de passe de l'emplacement réseau Insight.

  Même si vous désactivez ensuite le mode Insight dans l'interface utilisateur du périphérique, vous devez continuer à utiliser le mot de passe d'emplacement réseau Insight pour accéder à l'interface utilisateur du périphérique. Toutefois, vous pouvez modifier le mot de passe dans l'interface utilisateur du périphérique (voir Modifiez le mot de passe du compte utilisateur admin à la page 246).

REMARQUE: Lorsque Netgear insight gère AP, les paramètres des fonctionnalités que vous pouvez gérer via le portail cloud Insight et l'application Insight sont masqués dans l'interface utilisateur du terminal. Cependant, à l'aide de l'interface utilisateur du terminal, vous pouvez toujours gérer les paramètres de certaines fonctionnalités qui ne sont pas encore prises en charge dans Insight. En outre, les tâches de surveillance, de maintenance et de diagnostic restent disponibles dans l'interface utilisateur du périphérique.

Pour plus d'informations sur le fonctionnement du mot de passe réseau Insight et pour consulter des articles de la base de connaissances sur Netgear insight, visitez le site kb.netgear.com/000044338/.

Le tableau suivant répertorie les options d'informations d'identification pour l'accès à l'interface utilisateur du périphérique en relation avec le contrôleur d'engagement.

Table 2 : Informations d'identification pour l'accès au terminal lorsque APest intégré à un site engage Controller

Intégré à un site engage Controller	Informations d'identification	Menu de l'interface utilisateur du périphérique
Oui	Mot de passe du site du contrôleur d'engagement	Menu limité de l'interface utilisateur du périphérique.
Non, car vous avez retiré le AP du contrôleur d'engagement lors de la déconnexion duAP.*	Engagez le mot de passe du site du contrôleur jusqu'à ce que vous définissiez un nouveau mot de passe ou que vous réinitialisiez APles paramètres par défaut du	Menu limité de l'interface utilisateur du périphérique jusqu'à ce que vous réinitialisiez les paramètres par défaut duAP

* Si vous retirez le AP du contrôleur alors que le AP est en ligne, le AP est automatiquement réinitialisé aux paramètres par défaut.

Le tableau suivant répertorie les options d'informations d'identification essentielles pour l'accès à l'interface utilisateur du périphérique en relation avec Netgear insight.

Table 3 : Informations d'identification pour l'accès à l'interface utilisateur du terminal lorsque Netgear insight gère AP

Mode de gestion dans l'interface utilisateur du périphérique	Ajouté à un réseau Insight	Informations d'identification	Menu de l'interface utilisateur du périphérique
Mode Insight activé (paramètre par défaut)	Aucun	Mot de passe de l'administrateur du périphérique	Menu complet de l'interface utilisateur du périphérique
	Oui	Mot de passe réseau Insight	Menu limité de l'interface utilisateur du périphérique.

Table 3 : Informations d'identification pour l'accès à l'interface utilisateur du terminal lorsque Netgear insight gère AP (A continué)

Mode de gestion dans l'interface utilisateur du périphérique	Ajouté à un réseau Insight	Informations d'identification	Menu de l'interface utilisateur du périphérique
Mode Insight désactivé	Aucun	Mot de passe de l'administrateur du périphérique	Menu complet de l'interface utilisateur du périphérique
	Oui*	Mot de passe réseau Insight jusqu'à ce que vous définissiez un nouveau mot de passe	Menu complet de l'interface utilisateur du périphérique

* Cette situation se produit si vous désactivez le mode Insight après avoir déjà ajouté le AP à un emplacement réseau Insight.

Que faire si vous recevez un avertissement de sécurité du navigateur

Lorsque vous saisissez l'adresse IP attribuée à APdans le champ d'adresse de votre navigateur, un avertissement de sécurité peut s'afficher en raison du certificat auto-signé sur le terminal. Il s'agit d'un comportement attendu. Vous pouvez poursuivre ou ajouter une exception pour l'avertissement de sécurité.

Pour continuer avec un avertissement de sécurité ou ajouter une exception pour un avertissement de sécurité :

- Google Chrome Cliquez sur le lien **AVANCÉ**. Cliquez ensuite sur le lien **Proceed to x.x.x.x (non sécurisé)**, dans lequel x.x.x.x représente le nom de domaine ou l'adresse IP du périphérique.
- Apple Safari Cliquez sur le bouton **Afficher les détails**. Cliquez ensuite sur le lien **visiter ce site Web**. Si une fenêtre contextuelle d'avertissement s'affiche, cliquez sur le bouton **visiter le site Web**. Si une autre fenêtre contextuelle s'affiche pour vous permettre de confirmer les modifications apportées aux paramètres de confiance de votre certificat, entrez votre nom d'utilisateur Mac et votre mot de passe, puis cliquez sur le bouton **mettre à jour les paramètres**.

- Mozilla Firefox Cliquez sur le bouton **AVANCÉ**. Cliquez ensuite sur le bouton **Ajouter une exception**. Dans la fenêtre contextuelle qui s'affiche, cliquez sur le bouton **confirmer l'exception de sécurité**.
- Microsoft Edge Sélectionnez **Détails > aller à la page Web**.
- Microsoft Internet Explorer Cliquez sur le lien **continuer vers ce site Web (non recommandé)**.

4

Installez le AP sur un réseau WiFi maillé instantané Insight

En plus de fonctionner comme un point d'accès autonome normal, le AP peut fonctionner dans un réseau WiFi Insight instant Mesh en tant que racine AP (appelée *racine*) ou nœud (appelé *nœud*)AP.

Ce chapitre décrit comment utiliser le portail cloud Netgear insight ou l'application Insight pour connecter le système AP à une racine afin de permettre à ce dernier AP de fonctionner en tant que nœud dans un réseau Wi-Fi maillé instantané Insight. Le portail cloud Netgear insight et l'application Insight sont disponibles pour les abonnés Insight Premium et Insight Pro.

REMARQUE: Pour configurer un nœud dans un réseau WiFi maillé instantané Netgear insight avec une connexion à une racine, vous devez utiliser le portail cloud Netgear insight ou l'application Insight. Vous ne pouvez pas utiliser l'interface utilisateur de l'appareil pour configurer une connexion WiFi maillée vers une racine.

Pour plus d'informations sur la gestion et la surveillance du nœud avec le portail cloud Insight et l'application Insight, visitez le site netgear.com/insight. Le portail cloud Insight et l'application Insight intègrent une aide et sont documentés dans plusieurs articles de la base de connaissances auxquels vous pouvez accéder en visitant le site netgear.com/support.

Ce chapitre contient les sections suivantes :

- Qu'est-ce qu'une racine et un nœud ?
- Qu'est-ce qu'un réseau WiFi Insight instant Mesh ?
- Conditions requises pour placer un nœud dans un réseau WiFi Insight instant Mesh
- Accédez au portail Cloud pour configurer ou gérer un réseau WiFi Insight instant Mesh
- Connectez APen tant que nœud à une racine à l'aide de Cloud Portal

- Installez l'application Insight pour gérer un réseau WiFi maillé instantané Insight
- Connectez APen tant que nœud à une racine à l'aide de l'application Insight

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Qu'est-ce qu'une racine et un nœud ?

Le AP peut fonctionner dans un réseau WiFi à maillage instantané Insight en tant que racine ou nœud :

- Source Un réseau maillé APque vous configurez avec une connexion filaire à votre réseau pour créer une passerelle vers un ou plusieurs APréseaux maillés qui fonctionnent comme des nœuds. Sur la racine, utilisez le port Ethernet pour la connexion à votre réseau. Une racine peut desservir plusieurs nœuds simultanément.
- **Nœud**: Un réseau maillé APavec une connexion d'acheminement WiFi vers une racine qui fournit une connectivité Internet. Le nœud n'est pas connecté à votre réseau via une connexion filaire, mais via une connexion WiFi.

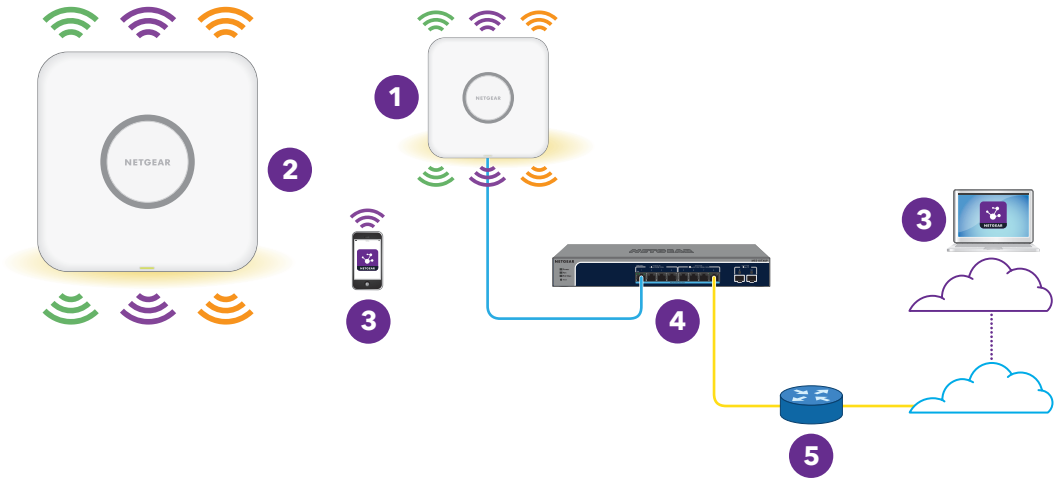

Illustration 7 : Réseau maillé avec un nœud et une racine filaire

Numéro ou icône et Description
1 Racine connectée via Ethernet à un commutateur réseau.
2 Nœud connecté à la racine via une connexion WiFi backhaul 6 GHz.
3 Un ordinateur ou une tablette avec accès au portail cloud Insight ou un téléphone mobile avec l'application Insight le portail cloud Insight ou l'application Insight vous permet de configurer et de gérer le nœud dans le réseau wifi maillé instantané Insight.
4 Un commutateur réseau.

(A continué)

Numéro ou icône et Description
5 Routeur réseau connecté à Internet.
Diffusion dans la bande radio 2,4 GHz.
Diffusion dans la bande radio 5 GHz.
Diffusion dans la bande radio 6 GHz.

Qu'est-ce qu'un réseau WiFi Insight instant Mesh ?

Un réseau wifi maillé se compose d'au moins une racine maillée et d'un ou plusieurs nœuds qui se connectent à la racine via WiFi (voir Qu'est-ce qu'une racine et un nœud ? à la page 60). La racine est connectée via Ethernet à un routeur ou à une passerelle Internet et fournit un accès Internet à ses nœuds. La racine et les nœuds fonctionnent ensemble pour couvrir une zone potentiellement étendue avec le réseau WiFi, à savoir le réseau maillé.

Un réseau maillé peut être une bonne solution si vous souhaitez intégrer le WiFi aux environnements suivants :

- Salles proches où le câblage n'est pas disponible (à portée de la vue et à portée de la réception WiFi actuelle)
- Immeubles de bureaux voisins (en visibilité directe et à portée de la réception WiFi actuelle)
- Tout environnement dans lequel vous ne pouvez pas exécuter de câbles

Dans le réseau WiFi maillé, le nœud se connecte à la racine via une connexion WiFi et diffuse (étend) le réseau WiFi aux clients WiFi :

- **Connexion backhaul** : La connexion WiFi entre la racine et le nœud est appelée connexion backhaul.
- **Liaison Fronthaul** : La connexion WiFi entre le nœud et ses clients WiFi est appelée connexion frontale.

Dans un réseau Wi-Fi maillé instantané Netgear insight, vous devez utiliser le portail cloud Insight ou l'application Insight pour configurer la connexion Wi-Fi maillée entre la racine et le nœud. Autrement dit, vous ne pouvez pas le faire via l'interface utilisateur du périphérique de la racine ou du nœud. Dans un réseau à racines multiples, Netgear insight connecte automatiquement le nœud à la racine ayant le signal WiFi le plus puissant.

Bien que le nœud diffuse le ou les mêmes réseaux WiFi que la racine, vous pouvez également configurer un réseau WiFi sur le nœud, qui peut ensuite être diffusé par la racine et les autres nœuds du réseau maillé.

Le AP peut diffuser sur la bande 2,4 GHz, la bande 5 GHz et la bande 6 GHz (la bande préférée pour la connexion backhaul sur le AP). Selon la capacité WiFi du client WiFi, n'importe quelle bande peut fournir la connexion frontale.

Conditions requises pour placer un nœud dans un réseau WiFi Insight instant Mesh

Les conditions requises pour placer un nœud dans un réseau WiFi Insight instant Mesh sont les suivantes :

- Le réseau WiFi existant doit inclure au moins un point d'accès maillé exécutant la dernière version du micrologiciel. Sur la racine, utilisez un port Ethernet pour la connexion à votre réseau.
- Le nœud doit être à l'état usine par défaut. Si vous avez déjà utilisé le nœud sur votre réseau, réinitialisez les paramètres par défaut duAP.
- Le nœud doit se trouver à portée du signal WiFi d'une racine afin qu'il puisse se synchroniser avec la racine. Lors de la configuration, pour une connexion WiFi fiable, placez le nœud à moins de 7,5 m (25 pieds), dans une ligne de mire avec un minimum d'obstacles par rapport à la racine la plus proche.
- Vous devez utiliser le portail cloud Netgear insight ou l'application Insight pour installer le nœud sur le réseau WiFi existant.

Pour plus d'informations sur les modèles de points d'accès NETGEAR pouvant fonctionner en tant que racine ou nœud, visitez le site kb.netgear.com/000065847.

Accédez au portail Cloud pour configurer ou gérer un réseau WiFi Insight instant Mesh

Le portail Insight Cloud est disponible pour les titulaires d'un abonnement Insight Premium ou Insight Pro.

Après avoir installé le AP sur un réseau Wi-Fi maillé instantané Insight, vous pouvez utiliser le portail cloud Insight pour configurer une connexion Wi-Fi maillée et configurer, gérer et surveiller le AP.

Pour plus d'informations sur le portail cloud Netgear insight, consultez les pages suivantes :

- netgear.com/fr/business/services/insight
- kb.netgear.com/fr/000061848
- kb.netgear.com/fr/000044338

Pour vous connecter à APvia Internet via le portail cloud Insight :

1. Sur un ordinateur ou une tablette, consultez le site insight.netgear.com.

   La page de connexion au compte NETGEAR s’affiche.
2. Si vous n’avez pas encore de compte Insight, vous pouvez en créer un maintenant.

   Pour plus d’informations sur la création d’un compte Insight Premium ou pour effectuer la mise à niveau vers un compte Insight Pro, consultez l’article kb.netgear.com/000044343.
3. Saisissez l'adresse e-mail et le mot de passe de votre compte NETGEAR, puis appuyez sur le bouton **NETGEAR Sign In** (Connexion NETGEAR).

Vous pouvez maintenant configurer la APconnexion WiFi maillée. Pour en savoir plus, consultez l'article kb.netgear.com/000061304.

Connectez APen tant que nœud à une racine à l'aide de Cloud Portal

Le portail Insight Cloud est disponible pour les titulaires d'un abonnement Insight Premium ou Insight Pro.

Vous pouvez utiliser le portail cloud Insight pour connecter APen tant que nœud à une racine. La racine doit être configurée avec une connexion filaire à un routeur ou à une passerelle Internet afin que la racine puisse fournir une connectivité Internet au nœud.

Pour plus d'informations sur le portail cloud Insight et les options de configuration et de gestion disponibles via le portail cloud Insight, visitez le site netgear.com/insight. Le portail cloud Insight intègre une aide et est documenté dans de nombreux articles de la base de connaissances auxquels vous pouvez accéder en visitant netgear.com/support.

Le nœud peut utiliser n'importe quelle bande pour établir la connexion backhaul à la racine et la connexion frontale aux clients WiFi. Cependant, une fois la connexion de liaison terrestre établie, si la racine et le nœud peuvent prendre en charge la bande de 6 GHz, le nœud bascule automatiquement sur la bande de 6 GHz comme bande préférée pour sa connexion de liaison terrestre. À l'aide du portail cloud Insight, vous pouvez modifier les paramètres de backhaul.

Pour utiliser le portail cloud Insight pour connecter le nœud à une racine d'un réseau WiFi existant :

1. Assurez-vous que le mode maillage de l'emplacement réseau Insight est défini sur Auto.

   Pour plus d'informations, visitez kb.netgear.com/000064932.
2. Assurez-vous que le mode maillage de la racine est défini sur Auto.

   Pour plus d'informations, visitez kb.netgear.com/000064931.
3. Assurez-vous que le nœud est à l'état usine par défaut.

   Si vous avez déjà utilisé le AP sur votre réseau, réinitialisez les paramètres par défaut duAP.
4. Pour une connexion WiFi fiable, placez le nœud à moins de 7,5 m (25 pieds), dans une ligne de mire, avec un minimum d'obstacles par rapport à la racine la plus proche.
5. Branchez le satellite à une source d'alimentation.

   Le voyant du nœud s'allume en orange, puis en vert.

   REMARQUE: Pour éviter une boucle réseau, connectez le nœud à un commutateur PoE++ qui *n'*est *pas* connecté au même réseau que la racine ou à Internet. Vous pouvez également utiliser un adaptateur secteur en option.
6. Accédez au portail cloud Insight en visitant le site insight.netgear.com, saisissez votre adresse e-mail et votre mot de passe NETGEAR, puis cliquez sur le bouton **connexion NETGEAR**.
7. Si vous utilisez uniquement Insight Pro, sélectionnez l'organisation à laquelle vous voulez ajouter le PR60X.

8. Sélectionnez l’emplacement où vous voulez ajouter le PA.
9. Cliquez sur le bouton **+ (Add Device)** (Ajouter un appareil).
10. Sur la page contextuelle Add New Device (Ajouter un nouvel appareil), saisissez le numéro de série du PR60X et l'adresse MAC, puis cliquez sur **Go** (Accéder).

    Insight détecte le nœud automatiquement. L'opération peut prendre quelques minutes.

    Le nœud tente de détecter et de se connecter à la racine qui fournit le signal WiFi le plus puissant sur le réseau WiFi maillé instantané Insight.

    REMARQUE: La connexion initiale et le processus de configuration peuvent prendre jusqu'à 10 minutes. Le nœud peut redémarrer pendant le processus de configuration.
11. Attendez que le nœud effectue la connexion initiale et le processus de configuration, que le voyant cesse de clignoter en orange, vert et bleu et qu'il s'allume en bleu fixe.

    REMARQUE: La connexion initiale et le processus de configuration peuvent prendre jusqu'à 10 minutes. Le nœud peut redémarrer pendant le processus de configuration.

    Le voyant s'allume comme suit pendant le processus de connexion et de configuration initial :

    - **Vert clignotant** : Le nœud tente de détecter une racine.
    - **Vert continu** : Le nœud établit sa première connexion avec la racine qui fournit le signal WiFi le plus puissant.
    - **Le voyant clignote lentement en orange** : Le nœud contacte le routeur réseau ou le serveur DHCP pour recevoir une adresse IP.

      Si le voyant ne cesse pas de clignoter en orange, reportez-vous à la section Le voyant clignote en orange lentement et en continu à la page 371.
    - **Orange, vert et bleu clignotants** : Le nœud est configuré en tant que périphérique géré dans le réseau WiFi maillé instantané Insight.

      Si le voyant ne cesse pas de clignoter en orange, vert et bleu, reportez-vous à la section Le voyant ne cesse pas de clignoter en orange, vert et bleu à la page 373.

    Lorsque la configuration est terminée, le voyant s'allume comme suit :

    - **Bleu continu** : La configuration est terminée et le nœud est prêt à fonctionner. Le nœud fonctionne dans le réseau WiFi maillé instantané Insight et est connecté au cloud Insight.

Le nœud est automatiquement configuré pour diffuser (étendre) le réseau WiFi de la racine.

Si vous rencontrez des difficultés pour connecter le nœud à une racine, reportez-vous à la section Le_nœud_et_la_racine_ne_peuvent_pas_se_connecter à la page 374.

Pour plus d'informations sur l'accès, la gestion et la surveillance du nœud à l'aide du portail cloud Netgear insight et de l'application Insight, visitez le site netgear.com/insight. Le portail cloud Insight et l'application Insight intègrent une aide et sont documentés dans plusieurs articles de la base de connaissances auxquels vous pouvez accéder en visitant le site netgear.com/support.

Installez l'application Insight pour gérer un réseau WiFi maillé instantané Insight

L'application Netgear insight est disponible pour les abonnés Insight Premium et Insight Pro.

Avant de pouvoir ajouter le AP à un réseau WiFi maillé instantané Insight à l'aide de l'application Netgear insight, vous devez installer l'application sur un périphérique mobile iOS ou Android.

Pour plus d'informations sur l'application Netgear insight, consultez les pages suivantes :

- netgear.com/fr/business/services/insight
- kb.netgear.com/fr/000061848
- kb.netgear.com/fr/000044338

Pour installer l'application Insight afin de gérer un réseau WiFi maillé instantané Insight :

1. Sur votre appareil mobile, rendez-vous dans la boutique d'applications, recherchez NETGEAR Insight et téléchargez la dernière version de l’application.

2. Lancez l'application Insight.

3. Si vous n’avez pas encore de compte Insight, vous pouvez en créer un maintenant.

   Pour plus d’informations sur la création d’un compte Insight Premium ou pour effectuer la mise à niveau vers un compte Insight Pro, consultez l’article kb.netgear.com/000044343.
4. Saisissez l'adresse électronique et le mot de passe de votre compte NETGEAR et appuyez sur **LOG IN** (Connexion).

Vous pouvez maintenant configurer la APconnexion WiFi maillée (voir Connectez APen tant que nœud à une racine à l'aide de l'application Insight à la page 67).

Connectez APen tant que nœud à une racine à l'aide de l'application Insight

Vous pouvez utiliser l'application Netgear insight pour connecter APen tant que nœud à une racine. La racine doit être configurée avec une connexion filaire à un routeur ou à une passerelle Internet afin que la racine puisse fournir une connectivité Internet au nœud.

Pour plus d'informations sur l'application Insight et les options de configuration et de gestion disponibles via l'application Insight, visitez le site netgear.com/insight. L'application Insight intègre une aide et est documentée dans plusieurs articles de la base de connaissances auxquels vous pouvez accéder en visitant netgear.com/support.

Le nœud peut utiliser n'importe quelle bande pour établir la connexion backhaul à la racine et la connexion frontale aux clients WiFi. Cependant, une fois la connexion de liaison terrestre établie, si la racine et le nœud peuvent prendre en charge la bande de 6 GHz, le nœud bascule automatiquement sur la bande de 6 GHz comme bande préférée pour sa connexion de liaison terrestre. À l'aide du portail cloud Insight, vous pouvez modifier les paramètres de backhaul.

Pour utiliser l'application Netgear insight pour connecter le nœud à une racine d'un réseau WiFi existant :

1. Assurez-vous que le mode maillage de l'emplacement réseau Insight est défini sur Auto.

   Pour plus d'informations, visitez kb.netgear.com/000064932.

Vous ne pouvez pas utiliser l'app Insight pour modifier le mode maillage de l'emplacement réseau Insight. Vous devez utiliser le portail Cloud. Pour toutes les autres étapes de cette procédure, vous *pouvez* utiliser l'app Insight.

2. Assurez-vous que le mode maillage de la racine est défini sur Auto.

   Pour plus d'informations, visitez kb.netgear.com/000064929.

3. Assurez-vous que le nœud est à l'état usine par défaut.

   Si vous avez déjà utilisé le AP sur votre réseau, réinitialisez les paramètres par défaut duAP.

4. Pour une connexion WiFi fiable, placez le nœud à moins de 7,5 m (25 pieds), dans une ligne de mire, avec un minimum d'obstacles par rapport à la racine la plus proche.
5. Branchez le satellite à une source d'alimentation.

   Le voyant du nœud s'allume en orange, puis en vert.

   REMARQUE: Pour éviter une boucle réseau, connectez le nœud à un commutateur PoE++ qui *n'*est *pas* connecté au même réseau que la racine ou à Internet. Vous pouvez également utiliser un adaptateur secteur en option.

6. Connectez votre appareil mobile au réseau WiFi existant qui inclut une ou plusieurs racines.
7. Lancez l'application Insight et connectez-vous à votre compte.
8. Sélectionnez l'emplacement réseau Insight avec la racine.

   Dans la plupart des cas, l'app Insight détecte automatiquement le nœud. L'opération peut prendre quelques minutes.

9. Effectuez l'une des opérations suivantes pour ajouter le nœud à l'emplacement réseau Insight :

   - **Détecté automatiquement** : Si le PA est détecté automatiquement et répertorié dans la section Insight Manageable Devices (Appareils manageables par Insight), appuyez sur l'icône AP (PA), puis sur le bouton **ADD DEVICE** (AJOUTER UN APPAREIL).
   - **Non détecté automatiquement** : Si le nœud n'est pas détecté automatiquement, procédez comme suit :

     a. Appuyez sur l'icône **+** dans la barre supérieure.

     b. Effectuez l'une des opérations suivantes :

- Appuyez sur le bouton **SCAN BARCODE OR QR CODE** (SCANNER LE CODE A BARRES OU LE CODE QR), puis scannez le code du PR60X.
- Appuyez sur le lien **Enter Serial Number and MAC Address** (Entrer le numéro de série et l'adresse MAC), puis saisissez manuellement le numéro de série et l'adresse MAC du PA.

c. Le cas échéant, nommez le PR60X et appuyez sur le bouton **Next** (Suivant).

Le nœud tente de détecter et de se connecter à la racine qui fournit le signal WiFi le plus puissant sur le réseau WiFi maillé instantané Insight.

REMARQUE: La connexion initiale et le processus de configuration peuvent prendre jusqu'à 10 minutes. Le nœud peut redémarrer pendant le processus de configuration.

10. Attendez que le nœud effectue la connexion initiale et le processus de configuration, que le voyant cesse de clignoter en orange, vert et bleu et qu'il s'allume en bleu fixe.

    REMARQUE: La connexion initiale et le processus de configuration peuvent prendre jusqu'à 10 minutes. Le nœud peut redémarrer pendant le processus de configuration.

    Le voyant s'allume comme suit pendant le processus de connexion et de configuration initial :

    - **Vert clignotant** : Le nœud tente de détecter une racine.
    - **Vert continu** : Le nœud établit sa première connexion avec la racine qui fournit le signal WiFi le plus puissant.
    - **Le voyant clignote lentement en orange** : Le nœud contacte le routeur réseau ou le serveur DHCP pour recevoir une adresse IP.

      Si le voyant ne cesse pas de clignoter en orange, reportez-vous à la section Le voyant clignote en orange lentement et en continu à la page 371.
    - **Orange, vert et bleu clignotants** : Le nœud est configuré en tant que périphérique géré dans le réseau WiFi maillé instantané Insight.

      Si le voyant ne cesse pas de clignoter en orange, vert et bleu, reportez-vous à la section Le voyant ne cesse pas de clignoter en orange, vert et bleu à la page 373.

    Lorsque la configuration est terminée, le voyant s'allume comme suit :

    - **Bleu continu** : La configuration est terminée et le nœud est prêt à fonctionner. Le nœud fonctionne dans le réseau WiFi maillé instantané Insight et est connecté au cloud Insight.

Le nœud est automatiquement configuré pour diffuser (étendre) le réseau WiFi de la racine.

Si vous rencontrez des difficultés pour connecter le nœud à une racine, reportez-vous à la section Le nœud et la racine ne peuvent pas se connecter à la page 374.

Pour plus d'informations sur l'accès, la gestion et la surveillance du nœud à l'aide du portail cloud Netgear insight et de l'application Insight, visitez le site netgear.com/insight. Le portail cloud Insight et l'application Insight intègrent une aide et sont documentés dans plusieurs articles de la base de connaissances auxquels vous pouvez accéder en visitant le site netgear.com/support.

5

Gérer les fonctions WiFi de base d'un réseau WiFi

Le AP peut prendre en charge huit réseaux WiFi, chacun avec ses propres paramètres WiFi, y compris la sécurité WiFi. Ce chapitre décrit comment gérer les fonctions WiFi de base d'un réseau WiFi.

Pour plus d'informations sur les fonctionnalités WiFi avancées d'un réseau WiFi, reportez-vous à la section Gérer les fonctions WiFi avancées d'un réseau WiFi à la page 313.

Ce chapitre comprend les sections suivantes :

- Configurez un réseau WiFi ouvert ou sécurisé
- Afficher ou modifier les paramètres d'un réseau WiFi
- Supprimer un réseau WiFi
- Masquer ou diffuser le SSID d'un réseau WiFi
- Modifiez l'ID VLAN d'un réseau WiFi
- Modifier l'authentification et la sécurité d'un réseau WiFi
- Activer ou désactiver PMF pour un réseau WiFi
- Configurez Multi PSK pour un réseau WiFi
- Activer ou désactiver un réseau WiFi ou configurer un programme d'activité WiFi
- Activer ou désactiver le guidage de bande
- Configurer l'opération multi-liens

REMARQUE: si vous souhaitez modifier les paramètres WiFi du routeur, utilisez une connexion filaire pour éviter d'être déconnecté lorsque les nouveaux paramètres WiFi prennent effet.

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Configurez un réseau WiFi ouvert ou sécurisé

Le AP fournit un SSID de configuration activé par défaut et qui diffuse sur la bande 2,4 GHz, la bande 5 GHz et la bande 6 GHz la GHz . Il s'agit du SSID que vous avez renommé et pour lequel vous avez défini une nouvelle phrase de passe lors de la connexion initiale au AP. Nous désignons également ce SSID comme réseau WiFi par défaut et il est affiché sous la forme SSID1 dans l'interface utilisateur du périphérique. Vous pouvez ajouter d'autres SSID : Le AP peut prendre en charge un total de huit SSID.

Le AP peut prendre en charge simultanément la bande 2,4 GHz pour les périphériques WiFi 802.11b/g/n/ax/Be, la bande 5 GHz pour les périphériques WiFi 802.11a/na/AC/ax/Be et la bande 6 GHz pour les périphériques 802.11ax/Be.

SSID signifie Service Set identifier, qui est le nom du réseau WiFi. Lorsque vous créez un nouveau SSID, vous définissez les paramètres d'un nouveau réseau WiFi, également appelé point d'accès virtuel (PAV). Cela signifie que le AP prend en charge jusqu'à huit réseaux WiFi ou points d'accès virtuels.

Si vous prévoyez d'utiliser la sécurité WPA2 Enterprise ou WPA3 Enterprise pour votre réseau WiFi, configurez d'abord les serveurs RADIUS (voir Configurer les serveurs RADIUS à la page 143). Notez que la sécurité WPA2 Enterprise et la sécurité WPA3 Enterprise ne sont pas compatibles avec une passerelle DNS multicast (mDNS) (voir Gérer la passerelle DNS multicast à la page 235).

Pour configurer un réseau WiFi invité :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner et d'ajouter un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Une page contextuelle affiche les paramètres du SSID.

6. Spécifiez le nom du réseau WiFi (SSID), indiquez si le SSID est diffusé et spécifiez l'ID VLAN comme décrit dans le tableau suivant.

Paramètre	Description
Nom du réseau sans fil (SSID)	Le SSID est le nom de réseau WiFi du PAV. Entrez un nom pour le SSID de 32 caractères maximum. Vous pouvez utiliser une combinaison de caractères alphanumériques et spéciaux, à l'exception des guillemets (") et d'une barre oblique inverse (\). Pour qu'un appareil WiFi puisse se connecter au PAV, le SSID de l'appareil WiFi doit correspondre au SSID du PAV.
Diffuser le SSID	Par défaut, le PAV diffuse son SSID afin que les clients WiFi puissent le détecter dans leurs listes de réseaux analysées. Pour désactiver la diffusion SSID, sélectionnez le bouton radio **non**. La désactivation de la diffusion SSID offre une sécurité WiFi supplémentaire, mais les utilisateurs doivent connaître le SSID pour pouvoir rejoindre le VAP.
Identifiant VLAN	Vous pouvez saisir l'ID VLAN qui doit être associé au PAVM. Par défaut, l'ID de gestion VLAN est 1. L'ID VLAN doit être compris entre 1 et 4094. Cet ID VLAN est différent de l'ID VLAN 802.1Q utilisé pour le réseau câblé (voir Définissez le VLAN de gestion et de VLAN 802.1Q à la page 224).

7. Spécifiez la sécurité WiFi en sélectionnant une option dans le menu **sécurité** et, le cas échéant, définissez une phrase de passe dans le champ **phrase de passe** ou sélectionnez une option dans le menu **cryptage** :

   - **Ouvrir**. Réseau WiFi ouvert qui n'offre aucune sécurité. Tout périphérique WiFi peut se connecter au réseau WiFi. Nous vous recommandons *de ne pas* utiliser un réseau WiFi ouvert existant mais de configurer la sécurité WiFi. Cependant, un réseau ouvert hérité peut être approprié pour un hotspot WiFi.

     Si vous sélectionnez **ouvrir** dans le menu **authentification**, la case à cocher **ouverture avancée** s'affiche.

     - **Case à cocher ouverture améliorée désactivée**: Le réseau WiFi est un réseau ouvert hérité sans aucune sécurité. Il s'agit de l'option par défaut pour un réseau ouvert. Les clients ne sont pas authentifiés, le trafic n'est pas chiffré et la norme 802.11w (PMF) est automatiquement désactivée (voir Étape 8).
     - **Case à cocher ouvrir améliorée sélectionnée**: La fonction d'ouverture Wi-Fi améliorée est activée. Cette fonctionnalité est basée sur le chiffrement sans fil opportuniste (OWE). Le cryptage est défini sur CCM mode Protocol (CCMP) et 802.11w (PMF) est automatiquement défini sur obligatoire (voir Étape 8).

       Si vous cochez la case **ouverture améliorée**, la case **autoriser les périphériques à se connecter avec ouverture** s'affiche.

       Si vous cochez la case **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi peut accepter les clients qui prennent en charge la fonction d'ouverture améliorée WiFi et les clients qui ne le prennent pas en charge. Pour les clients qui ne prennent pas en charge la fonction Wi-Fi Open Enhanced, le trafic n'est pas crypté.

       Dans ce cas, le nom SSID peut avoir une longueur maximale de 28 caractères. En outre, vous pouvez configurer un maximum de deux réseaux WiFi avec la sécurité OWE et la possibilité d'autoriser les clients qui prennent en charge la fonction ouverte améliorée WiFi et les clients qui ne le prennent pas en charge.

       Si vous désactivez la case à cocher **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi ne peut accepter que les clients qui prennent en charge la fonction d'ouverture améliorée WiFi.

   - **WPA2 personnel**: Cette option n'est pas disponible si la bande 6 GHz est activée.

     Cette option, identique à WPA2-PSK, utilise le cryptage AES. Ce type de sécurité permet uniquement aux périphériques WiFi qui prennent en charge WPA2 de rejoindre le VAP.

WPA2 fournit une connexion sécurisée, mais certains périphériques WiFi plus anciens ne détectent pas WPA2 et ne prennent en charge que WPA. Si votre réseau comprend de tels périphériques plus anciens, sélectionnez authentification **WPA2/WPA Personal**.

Dans le champ **phrase de passe**, saisissez une phrase de 8 à 63 caractères. Pour rejoindre le VAP, un utilisateur doit saisir cette phrase de passe. Pour afficher la phrase de passe en texte clair, cliquez sur l'icône en forme d'œil.

- **WPA2/WPA personnel**: Cette option n'est pas disponible si la bande 6 GHz est activée.

  Cette option, identique à WPA2-PSK/WPA-PSK, permet aux périphériques WiFi prenant en charge WPA2 ou WPA de rejoindre le PA2. Cette option utilise le cryptage AES et TKIP.

  WPA-PSK (qui utilise TKIP) est moins sécurisé que WPA2-PSK (qui utilise AES) et limite la vitesse des périphériques WiFi à 54 Mbit/s.

  Dans le champ **phrase de passe**, saisissez une phrase de 8 à 63 caractères. Pour rejoindre le VAP, un utilisateur doit saisir cette phrase de passe. Pour afficher la phrase de passe en texte clair, cliquez sur l'icône en forme d'œil.
- WPA2 ENTERPRISE Cette option n'est pas disponible si la bande 6 GHz est activée.

  Cette sécurité au niveau de l'entreprise utilise RADIUS pour la gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (AAA). Pour que la sécurité WPA2 Enterprise fonctionne, vous devez configurer des serveurs RADIUS (voir Configurer les serveurs RADIUS à la page 143).

  La sécurité WPA2 Enterprise et un portail captif s'excluent mutuellement.

  Dans le menu **cryptage**, sélectionnez le mode de cryptage des données :

  - **TKIP + AES**. Ce type de sécurité permet aux périphériques WiFi qui prennent en charge WPA ou WPA2 de se connecter au réseau WiFi du routeur. Il s'agit du mode par défaut.
  - AES Ce type de cryptage des données fournit une connexion sécurisée, mais certains appareils WiFi plus anciens ne détectent pas le WPA2 et ne prennent en charge que le WPA. Par conséquent, si votre réseau inclut de tels périphériques plus anciens, sélectionnez cryptage **TKIP + AES**.

  Lorsque vous sélectionnez authentification **WPA2 entreprise**, les boutons radio **VLAN dynamique** affichent :

- Activer. Le serveur RADIUS peut attribuer un ID VLAN aux clients. Si le serveur RADIUS ne le fait pas, les clients reçoivent automatiquement l'ID VLAN que vous avez configuré pour le SSID.
- Désactiver : Les clients se voient attribuer l'ID VLAN que vous avez configuré pour le SSID. Il s'agit de l'option par défaut.

Un VLAN dynamique s'exclut mutuellement avec un portail captif, un mode NAT, une isolation client sans fil, une passerelle DNS multicast (mDNS) et une opération multi-lien (MLO).

- **WPA3 personnel**: Cette option est l'option d'authentification personnelle la plus sécurisée. WPA3 utilise le cryptage SAE et permet uniquement aux périphériques WiFi prenant en charge WPA3 de rejoindre le VAP. Si vous sélectionnez cette option, 802.11w (PMF) est automatiquement défini sur obligatoire (voir Étape 8).

  WPA3 fournit une connexion sécurisée, mais certains périphériques WiFi plus anciens ne détectent pas WPA3 et ne prennent en charge que WPA. Si votre réseau inclut également des périphériques WPA2, sélectionnez authentification **WPA3/WPA2 personnelle**.

  Dans le champ **phrase de passe**, saisissez une phrase de 8 à 63 caractères. Pour rejoindre le VAP, un utilisateur doit saisir cette phrase de passe. Pour afficher la phrase de passe en texte clair, cliquez sur l'icône en forme d'œil.

- **WPA3/WPA2 personnel**: Cette option, identique à WPA3/WPA2-PSK, est le paramètre par défaut. Il permet aux périphériques WiFi prenant en charge le WPA3 ou le WPA2 de rejoindre le VAP. Cette option utilise le cryptage SAE et AES.

  WPA2-PSK (qui utilise AES) est moins sécurisé que WPA3 (qui utilise SAE).

  Dans le champ **phrase de passe**, saisissez une phrase de 8 à 63 caractères. Pour rejoindre le VAP, un utilisateur doit saisir cette phrase de passe. Pour afficher la phrase de passe en texte clair, cliquez sur l'icône en forme d'œil.

- WPA3 ENTERPRISE Cette sécurité au niveau de l'entreprise utilise RADIUS pour la gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (AAA). Pour que la sécurité WPA3 Enterprise fonctionne, vous devez configurer des serveurs RADIUS (voir Configurer les serveurs RADIUS à la page 143). Si vous sélectionnez cette option, 802.11w (PMF) est automatiquement défini sur obligatoire (voir Étape 8).

  La sécurité WPA3 Enterprise et un portail captif s'excluent mutuellement.

  Lorsque vous sélectionnez la sécurité WPA3 Enterprise, le cryptage est automatiquement défini sur GCMP256, qui est un protocole de cryptage de 256 bits.

Lorsque vous sélectionnez authentification **WPA3 entreprise**, les boutons radio **VLAN dynamique** affichent :

- Activer. Le serveur RADIUS peut attribuer un ID VLAN aux clients. Si le serveur RADIUS ne le fait pas, les clients reçoivent automatiquement l'ID VLAN que vous avez configuré pour le SSID.
- Désactiver : Les clients se voient attribuer l'ID VLAN que vous avez configuré pour le SSID. Il s'agit de l'option par défaut.

Un VLAN dynamique s'exclut mutuellement avec un portail captif, un mode NAT, une isolation client sans fil, une passerelle DNS multicast (mDNS) et une opération multi-lien (MLO).

8. Si vous le souhaitez, activez les trames de gestion protégées (PMF) 802.11w.

   Selon la norme 802.11w, Protected Management Frames (PMF) est une fonction de sécurité qui protège les trames de gestion unicast et multicast contre l'interception et la modification à des fins malveillantes. Le type d'authentification que vous sélectionnez détermine si cette fonctionnalité est obligatoire, facultative ou désactivée. Vous pouvez également le définir manuellement.

   - Obligatoire Cette option nécessite que les périphériques utilisent PMF. Les périphériques qui ne prennent pas en charge PMF ne peuvent pas se connecter au réseau WiFi. Si vous sélectionnez authentification ouverte améliorée, authentification personnelle WPA3 ou authentification entreprise WPA3, le bouton radio PMF est défini sur **obligatoire** et vous ne pouvez pas le modifier.
   - Facultatif : Cette option permet à d'APactiver automatiquement la fonction PMF selon que les terminaux peuvent la prendre en charge ou non. Si vous sélectionnez authentification personnelle WPA3/WPA2, le bouton radio PMF est défini sur **facultatif**, mais vous pouvez le modifier.
   - Désactiver : Cette option désactive PMF. Si vous sélectionnez l'authentification ouverte, WPA2 personnel, WPA2/WPA personnel ou WPA2 entreprise, le bouton radio PMF est défini sur **Désactivé**, mais vous pouvez le modifier (à l'exception de l'authentification ouverte).

9. Vous pouvez également activer Multi Pre-Shared Key (PSK), qui vous permet de séparer le réseau WiFi en différents VLAN, chacun accessible avec une phrase de passe unique.

   Multi PSK est pris en charge uniquement si la sécurité WiFi est WPA2 personnel ou WPA2/WPA personnel.

   Dans un sens, Multi PSK vous permet de créer différents sous-réseaux WiFi sur le réseau WiFi que vous configurez.

   Bien que vous puissiez également configurer cette fonctionnalité pendant la configuration d'un réseau WiFi, cette fonctionnalité est plus complexe et est donc

décrite séparément. Pour plus d'informations, consultez la section Configurez Multi PSK pour un réseau WiFi à la page 97.

10. Vous pouvez également désactiver la diffusion WiFi ou configurer un programme d'activité WiFi en sélectionnant l'un des boutons radio suivants :

    - **Toujours ALLUMÉ**: Lorsque vous configurez un SSID, vous créez un nouveau PAVM. Par défaut, le nouveau PAV est activé et le bouton radio **toujours ACTIVÉ** est sélectionné.
    - **Toujours DÉSACTIVÉ**: Sélectionnez ce bouton radio pour configurer le SSID mais désactiver temporairement le PAV.
    - Personnalisation Sélectionnez ce bouton radio pour configurer un programme de diffusion. Une icône s'affiche à droite du bouton radio. Effectuez les actions suivantes :

      a. Cliquez sur l'icône en regard du bouton radio.

         Une fenêtre contextuelle s'affiche.

      b. Sélectionnez une heure prédéfinie dans le menu **prédéfini** ou sélectionnez des plages horaires personnalisées en cliquant sur les plages horaires.

         Une couleur bleue pour un bloc horaire indique que le PAV sera activé (on). Une couleur grise pour un bloc horaire indique que le PAVM sera désactivé (désactivé).

      c. Cliquez sur **LE** bouton TERMINÉ.

         La fenêtre contextuelle se ferme.

      Pour chaque SSID, vous pouvez créer une planification personnalisée unique. Dans ce planning, pour chaque jour de minuit au lendemain de minuit, vous spécifiez l'heure ou les heures de désactivation du PAVM. Vous pouvez programmer un maximum de trois événements par jour.

11. Vous pouvez également sélectionner une ou deux bandes radio uniquement en désélectionnant une ou plusieurs cases à cocher.

    Décochez une ou plusieurs cases (2,4 GHz, 5 GHz ou 6 GHz) ou conservez la sélection par défaut. Par défaut, les cases 2,4 GHz et 5 GHz sont cochées, mais la case 6 GHz est décochée, ce qui signifie que le AP diffuse le SSID sur les bandes 2,4 GHz et 5 GHz.

    REMARQUE: Si vous activez la bande 6 GHz, seuls les clients WiFi prenant en charge les fonctionnalités WiFi 6 peuvent se connecter à la bande 6 GHz, ainsi qu'à la bande 2,4 GHz ou 5 GHz. Les clients WiFi qui ne prennent pas en charge les fonctionnalités WiFi 6 peuvent se connecter à la bande 2,4 GHz ou 5 GHz.

12. En option, activez le guidage de bande.

Par défaut, le guidage de bande est désactivé pour le PAV.

Pour activer le guidage de bande, sélectionnez le bouton radio **Activer**. Cela permet au AP, dans certaines conditions de canal, d'orienter les périphériques WiFi vers la bande 2,4 GHz, 5 GHz ou 6 GHz du PAV. Ces périphériques WiFi doivent être compatibles bi-bande ou tri-bande. Par rapport à la bande de 2,4 GHz, plus de canaux et de bande passante sont disponibles dans la bande de 5 GHz, et encore plus dans la bande de 6 GHz, causant moins d'interférences et permettant une meilleure expérience utilisateur.
La gestion du réseau WiFi 802.11k et RRM 802.11v affecte le réseau des manières suivantes :

- **802.11k RRM**: Cette fonction permet au AP et aux clients compatibles 802.11k de mesurer dynamiquement les ressources radio disponibles. Dans un réseau compatible 802.11k, APles s et les clients peuvent envoyer des rapports voisins, des rapports de balise et des rapports de mesure entre eux, ce qui permet aux clients compatibles 802.11k de sélectionner automatiquement le meilleur AP pour la connexion initiale ou le Roaming.
- **Gestion du réseau WiFi 802.11v** : Cette fonction permet au de AP diriger ses clients WiFi vers la bande 2,4 GHz, 5 GHz ou 6 GHz, en fonction de APla charge du canal du.

Le AP définit automatiquement le seuil de l'indicateur de puissance du signal reçu (RSSI). (Autrement dit, vous ne pouvez pas configurer le seuil RSSI manuellement.)

13. Vous pouvez également activer l'opération multi-liens (MLO).

    L'agrégation APdes radios du est appelée opération multi-liens (MLO), qui est une fonctionnalité clé de Wi-Fi 7. Les périphériques qui communiquent à l'aide de MLO sont appelés périphériques multiliens (MLD).

    Pour que MLO fonctionne, activez au moins deux radios et configurez le mode WiFi sur 11be pour chaque radio. . MLO améliore le débit, la latence et la fiabilité. Pour plus d'informations, consultez la section Configurer l'opération multi-liens à la page 105.

    Sous opération Multi-Link , sélectionnez l'un des boutons radio suivants :

    - Activer. MLO est activé. Les radios sur lesquelles 11be est activé sont regroupées pour fonctionner comme s'il s'agissait d'une liaison unique.
    - Désactiver : MLO est désactivé. Les radios sur lesquelles 11be est activé fonctionnent indépendamment. Il s'agit de l'option par défaut.

14. Pour définir le mode d'adressage et de trafic, configurer l'isolation des clients, configurer le suivi des URL, configurer un portail captif, sélectionner une liste de contrôle d'accès MAC pour les clients WiFi, configurer les limites de débit de bande passante, ou pour effectuer toutes ces opérations, faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

La page contextuelle se développe.

15. Vous pouvez également définir le mode NAT ou Bridge pour l'adressage et le trafic.

    Par défaut, le mode d'adressage et de trafic du AP est le mode Pont, ce qui signifie que les clients WiFi reçoivent des adresses IP d'un serveur DHCP (ou d'un routeur fonctionnant comme un serveur DHCP) de votre réseau. Il s'agit généralement du même serveur DHCP qui attribue une adresse IP au système AP lui-même.

    Vous pouvez également définir le mode NAT, qui active le APserveur DHCP du pour les clients WiFi. APLe serveur DHCP du système attribue une adresse IP dans une plage différente de l'adresse IP du système AP lui-même. Les modes NAT et Multi PSK (voir Étape 9) sont incompatibles.

    Dans le menu **adressage et trafic**, sélectionnez le mode adressage et trafic :

    REMARQUE: Cette option n'est pas prise en charge en Inde.

    - Bridge : Les clients WiFi reçoivent leurs adresses IP du serveur DHCP du même réseau que le AP. Il s'agit du mode par défaut.
    - NAT Les clients WiFi reçoivent leurs adresses IP d'un pool d'adresses DHCP privées sur le AP. Si vous sélectionnez ce mode, par défaut, l'adresse réseau WLAN est 172.31.0,0. Cela signifie que les clients WiFi se voient attribuer une adresse IP comprise entre 172.31.0.2 et 172.31.3,254. L'adresse IP du serveur DNS par défaut pour le WLAN est 8,8.8,8. Pour modifier la plage par défaut du pool d'adresses DHCP, du serveur DNS par défaut ou de la durée de bail, procédez comme suit :

      a. Dans le champ **adresse réseau** , saisissez une adresse réseau différente de celle du AP. Par exemple, si APl'adresse IP du système est comprise entre 192.168.0.1 et 192.168.0.254 (plage d'adresses IP courantes), saisissez une adresse réseau différente de 192.168.0,0.

      b. Dans le menu **masque de sous-réseau**, sélectionnez l'un des schémas de masque de sous-réseau préconfigurés.

      c. Dans le champ **DNS**, entrez l'adresse IP du serveur DNS que vous souhaitez utiliser. Cette adresse IP doit être différente de l'adresse réseau WLAN que vous avez définie à l'étape précédente.

      d. Dans le champ **Lease Time**, saisissez la période en minutes pendant laquelle le bail d'adresse est valide pour un client WiFi. La plage est de 5 minutes à 43200 minutes. La valeur par défaut est 1440 minutes (24 heures). Une fois le bail expiré, le client WiFi doit se reconnecter.

    Le mode NAT s'exclut mutuellement avec un VLAN dynamique (DVLAN), un PSK multiple (voir Étape 9), une passerelle DNS multicast (mDNS) et un VLAN de gestion autre que VLAN 1.

16. Vous pouvez également configurer l'isolation du client WiFi.

    Par défaut, l'isolation du client est désactivée pour le PAV et le bouton radio **désactiver** est sélectionné.

    Pour bloquer la communication entre les clients WiFi associés au même SSID ou à des SSID différents sur le AP, sélectionnez le bouton radio **Activer**.

    Lorsque vous sélectionnez le bouton radio **Activer**, la case **autoriser l'accès aux périphériques répertoriés ci-dessous** s'affiche. Vous pouvez ensuite sélectionner et ajouter des adresses IP statiques ou des domaines (qui se résolvent en adresses IP statiques) de périphériques réseau exemptés de l'isolation afin que les clients soient autorisés à les atteindre. Pour plus d'informations, consultez la section Activer ou désactiver l'isolation client pour un réseau WiFi à la page 317.

    L'isolation du client WiFi s'exclut mutuellement avec un groupe de filtre de trafic MAC/IP (voir Étape 22), un VLAN dynamique (DVLAN), un PSK multiple (voir Étape 9) et une passerelle DNS multicast (mDNS). Vous ne pouvez pas non plus activer l'isolation du client WiFi si vous interdisez le trafic de diffusion et de multidiffusion (voir Étape 21) ou si vous ne l'autorisez qu'à partir d'un groupe de périphériques spécifiques (voir Étape 22).

17. Si vous le souhaitez, activez le suivi des URL.

    Par défaut, le suivi des URL est désactivé et le bouton radio **désactiver** est sélectionné. Pour activer le suivi d'URL pour toutes les URL demandées par les clients WiFi connectés au SSID, sélectionnez le bouton radio **Activer**.

    Pour plus d'informations sur l'affichage des URL suivies par SSID ou par client WiFi, reportez-vous à la section Afficher ou télécharger les URL suivies à la page 306.

18. Pour configurer un portail captif, une ACL MAC pour les clients WiFi ou des limites de débit de bande passante, reportez-vous aux informations des sections suivantes :

    - Configurer et gérer un portail captif à la page 127
    - Gérer les listes de contrôle d'accès MAC pour les clients WiFi à la page 190 et Sélectionnez une liste de contrôle d'accès MAC pour les clients WiFi dans un réseau WiFi à la page 321
    - Définissez des limites de débit de bande passante pour un réseau WiFi à la page 324

    Bien que vous puissiez également configurer ces fonctions lors de la configuration d'un réseau WiFi, ces fonctions sont plus complexes et, par conséquent, décrites séparément.

19. Pour modifier les paramètres du message d'offre DHCP, autoriser ou interdire le trafic de diffusion et de multidiffusion, sélectionnez une liste de contrôle d'accès

MAC pour le trafic de diffusion et de multidiffusion des clients WiFi, sélectionnez un groupe de filtres de trafic MAC/IP ou effectuez toutes ces opérations, faites défiler vers le bas et cliquez sur l'onglet **>Traffic Policy**.

La page contextuelle se développe.

20. Vous pouvez également modifier les paramètres du message d'offre DHCP.

    Lorsqu'un terminal tente de s'associer au réseau WiFi et négocie une adresse IP, APconvertit le message d'offre DHCP de diffusion qu'il reçoit du serveur DHCP en message de monodiffusion, puis le transfère au terminal. Il s'agit de l'option par défaut (c'est-à-dire que le bouton radio **Activer** est sélectionné). Pour désactiver cette option afin que le système AP*ne* convertisse *pas* les messages d'offre DHCP de diffusion en messages monodiffusion, sélectionnez le bouton radio **désactiver**.

    Les paramètres du message d'offre DHCP ne sont pas disponibles et ne s'affichent pas sur la page si vous activez l'opération multi-lien (MLO, voir Étape 13).

21. Pour interdire le trafic de diffusion et de multidiffusion sur le réseau WiFi, décochez la case **autoriser le trafic de diffusion/multidiffusion**.

    Par défaut, le trafic broadcast et multicast est autorisé.

22. Pour sélectionner une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir de clients WiFi ou sélectionner un groupe de filtres de trafic MAC/IP, reportez-vous aux informations des sections suivantes :

    - Listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi à la page 198 et Sélectionnez une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi dans un réseau WiFi à la page 328
    - Gérer les groupes de filtres de trafic MAC/IP pour les réseaux WiFi à la page 205 et Sélectionnez un groupe de filtres de trafic MAC/IP pour un réseau WiFi à la page 332

    Bien que vous puissiez également configurer ces fonctions lors de la configuration d'un réseau WiFi, ces fonctions sont plus complexes et, par conséquent, décrites séparément.

23. Pour configurer la sélection avancée du débit pour la bande 2,4 GHz et la bande 5 GHz, faites défiler vers le bas et cliquez sur l'onglet **>sélection avancée du débit**.

    Pour plus d'informations, consultez la section Configurer la sélection avancée du débit pour un réseau WiFi à la page 334.

    Bien que vous puissiez également configurer cette fonction pendant la configuration d'un réseau WiFi, elle est plus complexe et, par conséquent, décrite séparément.

24. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

25. Assurez-vous qu'un client WiFi peut se connecter au nouveau réseau WiFi.

    Si le client ne parvient pas à se connecter au nouveau réseau WiFi, vérifiez les points suivants :

    - Si l'ordinateur ou l'appareil mobile compatible WiFi est déjà connecté à un autre réseau WiFi dans la zone, demandez à l'utilisateur de le déconnecter de ce réseau WiFi et de le connecter au réseau WiFi approprié. Certains périphériques WiFi se connectent automatiquement au premier réseau ouvert sans la sécurité WiFi qu'ils découvrent.
    - Si l'ordinateur ou le périphérique mobile WiFi tente de se connecter au réseau avec ses anciens paramètres (avant que l'utilisateur ne modifie les paramètres, demandez à l'utilisateur de mettre à jour la sélection de réseau WiFi dans l'ordinateur ou le périphérique mobile WiFi pour qu'elle corresponde aux paramètres actuels du réseau.
    - Le périphérique WiFi s'affiche-t-il comme un client connecté ? (Consultez la section Afficher la distribution des clients, les clients connectés et les tendances des clients à la page 296.) Si c'est le cas, il est connecté au réseau.
    - Utilisez-vous le nom de réseau (SSID) et le mot de passe corrects ?
    - Si l'authentification et le cryptage WiFi sont définis sur WPA3 personnel, assurez-vous que le pilote de l'adaptateur WiFi est mis à jour vers la dernière version sur l'ordinateur ou le périphérique mobile compatible WiFi.

Afficher ou modifier les paramètres d'un réseau WiFi

Vous pouvez afficher ou modifier les paramètres du réseau WiFi par défaut (SSID ou VAP) ou de tout réseau WiFi personnalisé. Le réseau WiFi par défaut est le SSID que vous avez renommé et pour lequel vous avez défini une nouvelle phrase de passe lors de votre connexion initiale au AP. Ce SSID s'affiche sous la forme SSID1 dans l'interface utilisateur du périphérique.

Pour afficher ou modifier les paramètres d'un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Modifiez les paramètres du réseau WiFi selon vos besoins.

   Pour obtenir une description détaillée des paramètres, reportez-vous à la section Configurez un réseau WiFi ouvert ou sécurisé à la page 73.

7. Si vous avez apporté des modifications, cliquez sur **le** bouton appliquer.

   Les paramètres sont enregistrés.

8. Si vous avez apporté des modifications, assurez-vous que vous pouvez vous reconnecter via WiFi au réseau avec ses nouveaux paramètres.

   Si vous ne parvenez pas à vous connecter via Wi-Fi, vérifiez les points suivants :

- Si l'ordinateur ou l'appareil mobile compatible WiFi est déjà connecté à un autre réseau WiFi dans la zone, demandez à l'utilisateur de le déconnecter de ce réseau WiFi et de le connecter au réseau WiFi approprié. Certains périphériques WiFi se connectent automatiquement au premier réseau ouvert sans la sécurité WiFi qu'ils découvrent.
- Si l'ordinateur ou le périphérique mobile WiFi tente de se connecter au réseau avec ses anciens paramètres (avant que l'utilisateur ne modifie les paramètres, demandez à l'utilisateur de mettre à jour la sélection de réseau WiFi dans l'ordinateur ou le périphérique mobile WiFi pour qu'elle corresponde aux paramètres actuels du réseau.
- Le périphérique WiFi s'affiche-t-il comme un client connecté ? (Consultez la section Afficher la distribution des clients, les clients connectés et les tendances des clients à la page 296.) Si c'est le cas, il est connecté au réseau.
- Utilisez-vous le nom de réseau (SSID) et le mot de passe corrects ?

Supprimer un réseau WiFi

Vous pouvez supprimer un réseau WiFi personnalisé (SSID ou VAP) dont vous n'avez plus besoin. Vous ne pouvez pas supprimer le réseau WiFi par défaut. Le réseau WiFi par défaut est le SSID que vous avez renommé et pour lequel vous avez défini une nouvelle phrase de passe lors de votre connexion initiale au AP. Ce SSID s'affiche sous la forme SSID1 dans l'interface utilisateur du périphérique.

Pour supprimer un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur l'icône de la corbeille à droite du SSID.

   Une fenêtre d'avertissement s'affiche.

6. Cliquez sur le bouton **Supprimer**.

   La fenêtre contextuelle se ferme et le réseau WiFi est supprimé.

Masquer ou diffuser le SSID d'un réseau WiFi

Par défaut, un réseau WiFi diffuse son nom de réseau WiFi (également appelé SSID) afin que les clients WiFi puissent détecter le SSID dans leurs listes de réseaux analysées. Pour plus de sécurité, vous pouvez désactiver la diffusion SSID et masquer le SSID afin que les utilisateurs doivent connaître le SSID pour pouvoir rejoindre le réseau WiFi.

REMARQUE: Si vous configurez un système de distribution sans fil (WDS ; voir Configurez un pont WiFi dans un système de distribution sans fil à la page 341), vous devez garder la diffusion SSID activée.

Pour masquer ou diffuser le nom de réseau d'un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.
5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.
6. Sous Broadcast SSID, sélectionnez l'un des boutons radio suivants :

- Non Le SSID est masqué pour le réseau WiFi.
- **Oui**: Le SSID est diffusé pour le réseau WiFi.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Modifiez l'ID VLAN d'un réseau WiFi

L'ID VLAN d'un réseau WiFi n'est pas le même que l'ID VLAN 802.1Q utilisé pour le réseau câblé (voir Définissez le VLAN de gestion et de VLAN 802.1Q à la page 224).

ATTENTION: Avant de modifier l'ID VLAN, assurez-vous que le VLAN est configuré sur le commutateur réseau et le serveur DHCP et que le AP et ses clients peuvent obtenir des adresses IP sur le nouveau VLAN.

Pour modifier l'ID VLAN d'un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Dans le champ **ID** (**ID VLAN**), entrez un ID (c'est-à-dire un nombre).

   Par défaut, l'ID VLAN d'un réseau WiFi est 1. L'ID VLAN doit être compris entre 1 et 4094.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Modifier l'authentification et la sécurité d'un réseau WiFi

Vous pouvez modifier l'authentification et le cryptage du réseau WiFi par défaut (SSID ou VAP) ou de tout réseau WiFi personnalisé. Le réseau WiFi par défaut est le SSID que vous avez renommé et pour lequel vous avez défini une nouvelle phrase de passe lors de votre connexion initiale au AP. Ce SSID s'affiche sous la forme SSID1 dans l'interface utilisateur du périphérique.

Avant de modifier l'authentification et le cryptage, réfléchissez aux types de clients qui doivent pouvoir se connecter au réseau WiFi. Le WPA3 fournit une connexion plus

sécurisée que le WPA2, mais certains périphériques WiFi peuvent ne pas encore détecter le WPA3 et ne prendre en charge que le WPA2. De même, le WPA2 fournit une connexion plus sécurisée que le WPA, mais certains périphériques WiFi existants ne détectent pas le WPA2 et ne prennent en charge que le WPA.

Si vous prévoyez d'utiliser la sécurité WPA2 Enterprise ou WPA3 Enterprise pour votre réseau WiFi, configurez d'abord les serveurs RADIUS (voir Configurer les serveurs RADIUS à la page 143).

Pour modifier l'authentification et la sécurité d'un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

La page qui s'affiche vous permet de sélectionner et d'ajouter un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Dans le menu **authentification**, sélectionnez l'un des types d'authentification suivants pour le réseau WiFi et, le cas échéant, définissez une nouvelle phrase de passe (clé réseau ou mot de passe WiFi) dans le champ **phrase de passe** ou sélectionnez une option dans le menu **cryptage** :

   - **Ouvrir**. Réseau WiFi ouvert qui n'offre aucune sécurité. Tout périphérique WiFi peut se connecter au réseau WiFi. Nous vous recommandons *de ne pas* utiliser un réseau WiFi ouvert existant mais de configurer la sécurité WiFi. Cependant, un réseau ouvert hérité peut être approprié pour un hotspot WiFi.

     Si vous sélectionnez **ouvrir** dans le menu **authentification**, la case à cocher **ouverture avancée** s'affiche.

     - **Case à cocher ouverture améliorée désactivée**: Le réseau WiFi est un réseau ouvert hérité sans aucune sécurité. Il s'agit de l'option par défaut pour un réseau ouvert. Les clients ne sont pas authentifiés, le trafic n'est pas chiffré et la norme 802.11w (PMF) est automatiquement désactivée (voir Activer ou désactiver PMF pour un réseau WiFi à la page 96).
     - **Case à cocher ouvrir améliorée sélectionnée**: La fonction d'ouverture Wi-Fi améliorée est activée. Cette fonctionnalité est basée sur le chiffrement sans fil opportuniste (OWE). Le cryptage est défini sur CCM mode Protocol (CCMP) et 802.11w (PMF) est automatiquement défini sur obligatoire (voir Activer ou désactiver PMF pour un réseau WiFi à la page 96). Si vous cochez la case **ouverture améliorée**, la case **autoriser les périphériques à se connecter avec ouverture** s'affiche.

       Si vous cochez la case **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi peut accepter les clients qui prennent en charge la fonction d'ouverture améliorée WiFi et les clients qui ne le prennent pas en charge. Pour les clients qui ne prennent pas en charge la fonction Wi-Fi Open Enhanced, le trafic n'est pas crypté.

       Dans ce cas, le nom SSID peut avoir une longueur maximale de 28 caractères. En outre, vous pouvez configurer un maximum de deux réseaux WiFi avec la sécurité OWE et la possibilité d'autoriser les clients qui prennent en charge la fonction ouverte améliorée WiFi et les clients qui ne le prennent pas en charge.

Si vous désactivez la case à cocher **autoriser les périphériques à se connecter avec l'ouverture**, le réseau WiFi ne peut accepter que les clients qui prennent en charge la fonction d'ouverture améliorée WiFi.

- **WPA2 personnel**: Cette option n'est pas disponible si la bande 6 GHz est activée.

  Cette option, identique à WPA2-PSK, utilise le cryptage AES. Ce type de sécurité permet uniquement aux périphériques WiFi qui prennent en charge WPA2 de rejoindre le VAP.

  WPA2 fournit une connexion sécurisée, mais certains périphériques WiFi plus anciens ne détectent pas WPA2 et ne prennent en charge que WPA. Si votre réseau comprend de tels périphériques plus anciens, sélectionnez authentification **WPA2/WPA Personal**.

  Dans le champ **phrase de passe**, saisissez une phrase de 8 à 63 caractères. Pour rejoindre le VAP, un utilisateur doit saisir cette phrase de passe. Pour afficher la phrase de passe en texte clair, cliquez sur l'icône en forme d'œil.

- **WPA2/WPA personnel**: Cette option n'est pas disponible si la bande 6 GHz est activée.

  Cette option, identique à WPA2-PSK/WPA-PSK, permet aux périphériques WiFi prenant en charge WPA2 ou WPA de rejoindre le PA2. Cette option utilise le cryptage AES et TKIP.

  WPA-PSK (qui utilise TKIP) est moins sécurisé que WPA2-PSK (qui utilise AES) et limite la vitesse des périphériques WiFi à 54 Mbit/s.

  Dans le champ **phrase de passe**, saisissez une phrase de 8 à 63 caractères. Pour rejoindre le VAP, un utilisateur doit saisir cette phrase de passe. Pour afficher la phrase de passe en texte clair, cliquez sur l'icône en forme d'œil.

- WPA2 ENTERPRISE Cette option n'est pas disponible si la bande 6 GHz est activée.

  Cette sécurité au niveau de l'entreprise utilise RADIUS pour la gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (AAA). Pour que la sécurité WPA2 Enterprise fonctionne, vous devez configurer des serveurs RADIUS (voir Configurer les serveurs RADIUS à la page 143).

  La sécurité WPA2 Enterprise et un portail captif s'excluent mutuellement.

  Dans le menu **cryptage**, sélectionnez le mode de cryptage des données :

  - **TKIP + AES**. Ce type de sécurité permet aux périphériques WiFi qui prennent en charge WPA ou WPA2 de se connecter au réseau WiFi du routeur. Il s'agit du mode par défaut.
  - AES Ce type de cryptage des données fournit une connexion sécurisée, mais certains appareils WiFi plus anciens ne détectent pas le WPA2 et ne prennent

en charge que le WPA. Par conséquent, si votre réseau inclut de tels périphériques plus anciens, sélectionnez cryptage **TKIP + AES**.

Lorsque vous sélectionnez authentification **WPA2 entreprise**, les boutons radio **VLAN dynamique** affichent :

- Activer. Le serveur RADIUS peut attribuer un ID VLAN aux clients. Si le serveur RADIUS ne le fait pas, les clients reçoivent automatiquement l'ID VLAN que vous avez configuré pour le SSID.
- Désactiver : Les clients se voient attribuer l'ID VLAN que vous avez configuré pour le SSID. Il s'agit de l'option par défaut.

Un VLAN dynamique s'exclut mutuellement avec un portail captif, un mode NAT, une isolation client sans fil, une passerelle DNS multicast (mDNS) et une opération multi-lien (MLO).

- **WPA3 personnel**: Cette option est l'option d'authentification personnelle la plus sécurisée. WPA3 utilise le cryptage SAE et permet uniquement aux périphériques WiFi prenant en charge WPA3 de rejoindre le VAP. Si vous sélectionnez cette option, 802.11w (PMF) est automatiquement défini sur obligatoire (voir Activer ou désactiver PMF pour un réseau WiFi à la page 96).

  WPA3 fournit une connexion sécurisée, mais certains périphériques WiFi plus anciens ne détectent pas WPA3 et ne prennent en charge que WPA. Si votre réseau inclut également des périphériques WPA2, sélectionnez authentification **WPA3/WPA2 personnelle**.

  Dans le champ **phrase de passe**, saisissez une phrase de 8 à 63 caractères. Pour rejoindre le VAP, un utilisateur doit saisir cette phrase de passe. Pour afficher la phrase de passe en texte clair, cliquez sur l'icône en forme d'œil.

- **WPA3/WPA2 personnel**: Cette option, identique à WPA3/WPA2-PSK, est le paramètre par défaut. Il permet aux périphériques WiFi prenant en charge le WPA3 ou le WPA2 de rejoindre le VAP. Cette option utilise le cryptage SAE et AES.

  WPA2-PSK (qui utilise AES) est moins sécurisé que WPA3 (qui utilise SAE).

  Dans le champ **phrase de passe**, saisissez une phrase de 8 à 63 caractères. Pour rejoindre le VAP, un utilisateur doit saisir cette phrase de passe. Pour afficher la phrase de passe en texte clair, cliquez sur l'icône en forme d'œil.

- WPA3 ENTERPRISE Cette sécurité au niveau de l'entreprise utilise RADIUS pour la gestion centralisée de l'authentification, de l'autorisation et de la comptabilité (AAA). Pour que la sécurité WPA3 Enterprise fonctionne, vous devez configurer des serveurs RADIUS (voir Configurer les serveurs RADIUS à la page 143). Si vous sélectionnez cette option, 802.11w (PMF) est automatiquement défini sur obligatoire (voir Activer ou désactiver PMF pour un réseau WiFi à la page 96).

La sécurité WPA3 Enterprise et un portail captif s'excluent mutuellement.

Lorsque vous sélectionnez la sécurité WPA3 Enterprise, le cryptage est automatiquement défini sur GCMP256, qui est un protocole de cryptage de 256 bits.

Lorsque vous sélectionnez authentification **WPA3 entreprise**, les boutons radio **VLAN dynamique** affichent :

- Activer. Le serveur RADIUS peut attribuer un ID VLAN aux clients. Si le serveur RADIUS ne le fait pas, les clients reçoivent automatiquement l'ID VLAN que vous avez configuré pour le SSID.
- Désactiver : Les clients se voient attribuer l'ID VLAN que vous avez configuré pour le SSID. Il s'agit de l'option par défaut.

Un VLAN dynamique s'exclut mutuellement avec un portail captif, un mode NAT, une isolation client sans fil, une passerelle DNS multicast (mDNS) et une opération multi-lien (MLO).

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

8. Assurez-vous qu'un client WiFi peut se connecter au nouveau réseau WiFi.

   Si le client ne parvient pas à se connecter au nouveau réseau WiFi, vérifiez les points suivants :

   - Si l'ordinateur ou l'appareil mobile compatible WiFi est déjà connecté à un autre réseau WiFi dans la zone, demandez à l'utilisateur de le déconnecter de ce réseau WiFi et de le connecter au réseau WiFi approprié. Certains périphériques WiFi se connectent automatiquement au premier réseau ouvert sans la sécurité WiFi qu'ils découvrent.
   - Si l'ordinateur ou le périphérique mobile WiFi tente de se connecter au réseau avec ses anciens paramètres (avant que l'utilisateur ne modifie les paramètres, demandez à l'utilisateur de mettre à jour la sélection de réseau WiFi dans l'ordinateur ou le périphérique mobile WiFi pour qu'elle corresponde aux paramètres actuels du réseau.
   - Le périphérique WiFi s'affiche-t-il comme un client connecté ? (Consultez la section Afficher la distribution des clients, les clients connectés et les tendances des clients à la page 296.) Si c'est le cas, il est connecté au réseau.
   - Utilisez-vous le nom de réseau (SSID) et le mot de passe corrects ?
   - Si vous avez modifié l'authentification WiFi et le cryptage en WPA3 personnel, assurez-vous que le pilote de l'adaptateur WiFi est mis à jour vers la dernière version sur votre ordinateur ou périphérique mobile compatible WiFi.

Activer ou désactiver PMF pour un réseau WiFi

Selon la norme 802.11w, Protected Management Frames (PMF) est une fonction de sécurité qui protège les trames de gestion unicast et multicast contre l'interception et la modification à des fins malveillantes. Le type d'authentification que vous sélectionnez détermine si cette fonctionnalité est obligatoire, facultative ou désactivée. Vous pouvez également le définir manuellement.

Pour activer ou désactiver PMF pour un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Sous 802.11w (PMF), sélectionnez l'un des boutons radio suivants :
   - Obligatoire Nécessite que les périphériques utilisent PMF. Les périphériques qui ne prennent pas en charge PMF ne peuvent pas se connecter au réseau WiFi. Si vous sélectionnez authentification ouverte améliorée, authentification personnelle WPA3 ou authentification entreprise WPA3, le bouton radio PMF est défini sur **obligatoire** et vous ne pouvez pas le modifier.
   - Facultatif : Permet à d' APd'activer automatiquement la fonction PMF selon que les terminaux prennent en charge la fonction PMF ou non. Si vous sélectionnez authentification personnelle WPA3/WPA2, le bouton radio PMF est défini sur **facultatif**, mais vous pouvez le modifier.
   - Désactiver : PMF est désactivé pour le réseau WiFi. Si vous sélectionnez l'authentification ouverte, WPA2 personnel, WPA2/WPA personnel ou WPA2 entreprise, le bouton radio PMF est défini sur **Désactivé**, mais vous pouvez le modifier (à l'exception de l'authentification ouverte).

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Configurez Multi PSK pour un réseau WiFi

La clé multi-pré-partagée (PSK) est prise en charge uniquement si la sécurité WiFi est WPA2 personnel ou WPA2/WPA personnel.

Multi PSK (MPSK) vous permet de séparer un seul réseau WiFi en différents VLAN, chacun accessible avec une phrase de passe unique. Dans un sens, Multi PSK vous permet de créer différents sous-réseaux WiFi sur un seul réseau WiFi. Lors de la connexion au réseau WiFi, la phrase de passe saisie par l'utilisateur détermine le VLAN dans lequel le client WiFi est placé.

Outre une VLAN et une phrase de passe, vous pouvez associer un identificateur de clé au mappage VLAN-à-phrase de passe. L'identificateur de clé vous permet d'identifier

les VLAN du réseau WiFi à des fins de surveillance du réseau. Par exemple, lorsque vous affichez des clients WiFi, l'identifiant de clé peut également s'afficher.

Comme exemples d'identificateurs de clé, vous pouvez utiliser des termes tels que corporatenetwork_22, corporatenetwork_23 et corporatenetwork_24. Ces identifiants de clé (ou les identifiants VLAN associés) ne sont pas visibles par un utilisateur qui tente de se connecter au réseau WiFi : l'utilisateur voit le SSID et saisit la phrase de passe.

Si vous activez Multi PSK, la phrase de passe et le VLAN du réseau WiFi sont remplacés par les phrases de passe et les VLAN qui font partie de la configuration Multi PSK.

REMARQUE: Pour configurer Multi PSK sur le réseau WiFi par défaut (affiché sous la forme SSID1 dans l'interface utilisateur du terminal), qui est le réseau WiFi que vous avez défini lors de la connexion initiale à AP, vous devez d'abord définir la sécurité WiFi sur WPA2 personnel ou WPA2/WPA personnel.

En outre, les restrictions suivantes s'appliquent à Multi PSK :

- Vous ne pouvez pas activer Multi PSK pour un réseau WiFi dans la bande de 6 GHz.
- Vous pouvez configurer Multi PSK sur un maximum de quatre réseaux WiFi sur un point d'accès.
- Chaque réseau WiFi sur lequel vous configurez Multi PSK peut prendre en charge un maximum de huit mappages VLAN-phrase de passe. (Au sein de chaque réseau WiFi, chaque phrase de passe et chaque identificateur de clé doit être unique.) Un point d'accès peut prendre en charge un maximum de 400 mappages VLAN/phrase de passe multi PSK. Par exemple, quatre réseaux WiFi peuvent chacun prendre en charge huit mappages VLAN/phrase de passe multi PSK.

  REMARQUE: Si vous gérez le AP à l'aide de Insight, chaque réseau WiFi sur lequel vous configurez Multi PSK peut prendre en charge un maximum de 1000 mappages VLAN-à-phrase de passe.
- Dans un PSK multiple sur un réseau WiFi unique, vous pouvez mapper le même ID VLAN à différentes phrases de passe. Vous pouvez également utiliser le même ID VLAN pour plusieurs PSK sur différents réseaux WiFi.
- Si le routage inter-VLAN est désactivé dans le réseau auquel un point d'accès est connecté, les conditions suivantes s'appliquent :
  - Les clients WiFi connectés à différents VLAN sur le même réseau WiFi (c'est-à-dire que les clients WiFi utilisent des phrases de passe différentes pour se connecter au même réseau WiFi) ne peuvent pas communiquer entre eux et restent isolés.
  - Les clients WiFi connectés au *même* VLAN sur différents réseaux WiFi *peuvent* communiquer entre eux.
- Multi PSK et les fonctionnalités suivantes s'excluent mutuellement :

- Opération Multi-Link (voir Configurer l'opération multi-liens à la page 105)
- Portail captif (voir Configurer et gérer un portail captif à la page 127)
- Passerelle mDNS (voir Gérer la passerelle DNS multicast à la page 235)
- Mode NAT (voir Définissez le mode NAT ou Bridge pour l'adressage et le trafic à la page 315)
- Isolation du client (voir Activer ou désactiver l'isolation client pour un réseau WiFi à la page 317)

Pour configurer Multi PSK pour un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

   Vous ne pouvez pas configurer Multi PSK sur le réseau WiFi par défaut (affiché sous la forme SSID1 dans l'interface utilisateur du terminal), qui est le réseau WiFi que vous avez défini lors de la connexion initiale à AP.

6. Sélectionnez le bouton radio Multi PSK **Enable**.

   La page s'ajuste.

7. Configurez les paramètres Multi PSK :

   a. Pour ajouter une nouvelle entrée Multi PSK, spécifiez les paramètres suivants :

      - Identifiant VLAN : ID VLAN, qui correspond à l'VLAN dont un client WiFi devient membre.

        L'ID VLAN doit être compris entre 1 et 4094.

      - Phrase d'authentification : Phrase de passe unique (mot de passe WiFi) qu'un utilisateur doit saisir pour permettre au client WiFi de se connecter au VLAN associé du réseau WiFi.

        La phrase de passe doit comporter entre 8 et 63 caractères.

      - Identificateur de clé Nom ou expression permettant d'identifier le VLAN dans le réseau WiFi à des fins de surveillance. La longueur maximale est de 30 caractères alphanumériques, y compris les caractères spéciaux suivants : trait d'Union (-) et trait de soulignement (_).

      - **Isolement du groupe par rapport aux autres groupes**: Pour activer ce paramètre, cliquez sur le bouton pour qu'il s'affiche en bleu.

        Pour plus de sécurité, vous pouvez activer le bouton isolation de groupe à partir d'autres groupes afin que les clients associés au même réseau puissent uniquement communiquer entre eux, et non avec des clients extérieurs à ce réseau.

   b. Pour ajouter une autre entrée Multi PSK, cliquez sur le bouton **+** à gauche de Ajouter une nouvelle phrase de passe et répétez l'étape précédente a.

   c. Pour supprimer une entrée Multi PSK, cliquez sur l'icône de la corbeille à droite de l'entrée.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer ou désactiver un réseau WiFi ou configurer un programme d'activité WiFi

Vous pouvez désactiver temporairement un réseau WiFi (SSID ou VAP), vous pouvez le réactiver ou configurer un calendrier spécifiant quand le réseau WiFi est actif.

Programmation d'un réseau WiFi fonctionnalité verte qui vous permet de désactiver le réseau WiFi pendant les vacances programmées, les fermetures de bureaux, le soir ou le week-end.

Pour chaque SSID, vous pouvez créer une planification personnalisée unique. Dans ce planning, pour chaque jour de minuit au lendemain de minuit, vous spécifiez l'heure ou les heures de désactivation du PAVM. Vous pouvez programmer un maximum de trois événements par jour.

Pour désactiver ou activer un réseau WiFi ou configurer un programme d'activité WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.
5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.
6. Sous Planning, sélectionnez l'un des boutons radio suivants :

   - **Toujours ALLUMÉ**: Le réseau WiFi est activé.
   - **Toujours DÉSACTIVÉ**: Le réseau WiFi est désactivé.
   - Personnalisation Le réseau WiFi est activé ou désactivé selon un calendrier que vous devez configurer.
     Une icône s'affiche à droite du bouton radio.
7. Si vous avez sélectionné **personnalisé** à l'étape précédente, procédez comme suit :

   a. Cliquez sur l'icône en regard du bouton radio.

      Une fenêtre contextuelle s'affiche.

   b. Sélectionnez une heure prédéfinie dans le menu **prédéfini** ou sélectionnez des plages horaires personnalisées en cliquant sur les plages horaires.
      Une couleur bleue pour un bloc horaire indique que le réseau WiFi sera activé (activé). Une couleur grise pour un bloc horaire indique que le réseau WiFi sera désactivé (désactivé).

   c. Cliquez sur **LE** bouton TERMINÉ.

La fenêtre contextuelle se ferme.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer ou désactiver le guidage de bande

L'orientation de bande permet au système AP d'identifier les périphériques WiFi compatibles bi-bande ou tri-bande et de les orienter vers la bande 2,4 GHz, 5 GHz ou 6 GHz d'un réseau WiFi (SSID ou VAP). Par rapport à la bande de 2,4 GHz, plus de canaux et de bande passante sont disponibles dans la bande de 5 GHz, et encore plus dans la bande de 6 GHz, causant moins d'interférences et permettant une meilleure expérience utilisateur. L'orientation des bandes inclut la gestion des ressources radio (RRM) 802.11k et la gestion du réseau WiFi 802.11v. Par défaut, le guidage de bande est désactivé.

La gestion du réseau WiFi 802.11k et RRM 802.11v affecte le réseau des manières suivantes :

- **802.11k RRM**: Cette fonction permet au AP et aux clients compatibles 802.11k de mesurer dynamiquement les ressources radio disponibles. Dans un réseau compatible 802.11k, APles s et les clients peuvent envoyer des rapports voisins, des rapports de balise et des rapports de mesure entre eux, ce qui permet aux clients compatibles 802.11k de sélectionner automatiquement le meilleur AP pour la connexion initiale ou le Roaming.
- **Gestion du réseau WiFi 802.11v** : Cette fonction permet au de AP diriger ses clients WiFi vers la bande 2,4 GHz, 5 GHz ou 6 GHz, en fonction de APla charge du canal du. Dans un environnement avec plusieurs APs, la gestion du réseau WiFi 802.11v aide les clients WiFi en itinérance à sélectionner le meilleur AP.

Le AP définit automatiquement le seuil de l'indicateur de puissance du signal reçu (RSSI). (Autrement dit, vous ne pouvez pas configurer le seuil RSSI manuellement.)

Pour activer ou désactiver le guidage de bande :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations,

consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l'appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s'affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Sous Band Steering, sélectionnez l'un des boutons radio suivants :

   - Désactiver : Le guidage de bande est désactivé pour le PAV. Il s'agit de l'option par défaut.
   - Activer. Dans certaines conditions de canal, le AP oriente les périphériques WiFi vers la bande 2,4 GHz, 5 GHz ou 6 GHz du PAV. Ces périphériques WiFi doivent être compatibles bi-bande ou tri-bande.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Configurer l'opération multi-liens

L'agrégation APdes radios du est appelée opération multi-liens (MLO), qui est une fonctionnalité clé de Wi-Fi 7. Les périphériques qui communiquent à l'aide de MLO sont appelés périphériques multiliens (MLD).

Pour que MLO fonctionne, activez au moins deux radios et configurez le mode WiFi sur 11be pour chaque radio.

MLO améliore le débit, la latence et la fiabilité :

- Les périphériques WiFi ne sont plus limités à fonctionner sur un seul canal de la radio 2,4 GHz, 5 GHz ou 6 GHz, mais peuvent désormais utiliser plusieurs liaisons sur des bandes de fréquence.
- MLO simultané permet d'agréger le trafic sur plusieurs radios, ce qui entraîne les résultats suivants :
  - Débit maximal et faible latence
  - Trafic commuté de manière dynamique entre les bandes radio pour éviter les interférences WiFi
  - Faible latence déterministe et prévisible même dans les environnements fortement encombrés

Par défaut, MLO est désactivé. L'activation de MLO permet aux clients compatibles MLO d'envoyer du trafic sur plusieurs bandes en même temps.

MLO et les fonctionnalités suivantes sont mutuellement incompatibles :

- Listes de contrôle d'accès MAC pour les réseaux WiFi (voir Gérer les listes de contrôle d'accès MAC pour les clients WiFi à la page 190 et Listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi à la page 198)
- Multi PSK (voir Configurez Multi PSK pour un réseau WiFi à la page 97)
- Sécurité WPA2 entreprise et sécurité WPA3 entreprise utilisant un réseau VLAN dynamique (DVLAN, voir Configurez un réseau WiFi ouvert ou sécurisé à la page 73 et Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90)

Pour configurer une opération multi-liens :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l'appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s'affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Sous opération Multi-Link , sélectionnez l'un des boutons radio suivants :

   - Activer. MLO est activé. Les radios sur lesquelles 11be est activé sont regroupées pour fonctionner comme s'il s'agissait d'une liaison unique.
   - Désactiver : MLO est désactivé. Les radios sur lesquelles 11be est activé fonctionnent indépendamment. Il s'agit de l'option par défaut.

   ATTENTION: Après avoir cliqué sur le bouton appliquer, tous les clients WiFi sont temporairement déconnectés avant d'être automatiquement reconnectés.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

6

Gérer les fonctions de base de la radio

Ce chapitre décrit comment gérer les fonctions radio de base du AP. Pour plus d'informations sur les fonctions radio avancées, reportez-vous à la section Gérer les fonctions avancées de la radio à la page 347.

ATTENTION: Si vous modifiez une fonction radio sur la radio 2,4 GHz, la modification affecte tous les réseaux WiFi diffusant sur la radio 2,4 GHz. De même, si vous modifiez une fonction radio sur la radio 5 GHz ou 6 GHz, la modification affecte tous les réseaux WiFi diffusant sur la radio 5 GHz ou 6 GHz. Si la modification n'est pas spécifique à une radio, elle affecte *tous les* réseaux WiFi sur le AP.

Ce chapitre comprend les sections suivantes :

- Gérez les paramètres WiFi de base des radios
- Permet d'allumer ou d'éteindre une radio
- Permet de modifier le mode préambule d'une radio
- Permet de changer de canal pour une radio
- Modifier l'intervalle de garde d'une radio
- Modifier la puissance de sortie d'une radio
- Permet de changer de canal pour une radio
- Gérer la qualité de service pour une radio WiFi

REMARQUE: si vous souhaitez modifier les paramètres WiFi du routeur, utilisez une connexion filaire pour éviter d'être déconnecté lorsque les nouveaux paramètres WiFi prennent effet.

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Gérez les paramètres WiFi de base des radios

Les paramètres WiFi de base de chaque radio s'appliquent à tous les réseaux WiFi (VPN ou SSID) configurés sur la radio. Vous pouvez spécifier les paramètres radio pour les radios de bande 2,4 GHz, 5 GHz et 6 GHz individuellement.

Pour gérer les paramètres WiFi de base des radios :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page Paramètres sans fil s'affiche et affiche les mêmes types de paramètres pour chaque radio.

   Les descriptions suivantes s'appliquent à toutes les radios, mais vous pouvez spécifier les paramètres radio pour les radios 2,4 GHz, 5 GHz et 6 GHz individuellement.

5. Gardez ou éteignez une radio :

   - **Case Activer la radio cochée**: Par défaut, la case **Activer la radio** est cochée et la radio diffuse.
   - **Case à cocher ACTIVER la radio désactivée**: La désactivation d'une radio désactive l'accès WiFi pour la bande, ce qui peut être utile lors de la configuration, du réglage du réseau ou du dépannage.

6. Sélectionnez l'un des boutons radio **mode sans fil** suivants pour une radio, ce qui détermine si vous pouvez définir la largeur de canal et, le cas échéant, quelles sont les largeurs de canal disponibles :

   - 2,4 GHz
     - 11be : Les clients WiFi 802.11be, 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Il s'agit de l'option par défaut.
     - 11ax : Les clients WiFi 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Il s'agit de l'option par défaut.
     - 11 ng Les clients WiFi 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11ax est limitée à la vitesse maximale prise en charge par 802.11ng (environ 450 Mbit/s).
     - 11bg : Les clients WiFi 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11ax et 802.11ng est limitée à la vitesse maximale prise en charge par 802.11bg (environ 54 Mbit/s).
     - 11b : Les clients WiFi 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11ax, 802.11n et 802.11bg est limitée à la vitesse maximale prise en charge par 802.11b (environ 11 Mbit/s).
   - 5 GHz
     - 11be : Les clients WiFi 802.11be, 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès. Il s'agit de l'option par défaut.
     - 11ax : Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès.

- 11ac : Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11be et 802.11ax est limitée à la vitesse maximale prise en charge par 802.11ac (environ 867 Mbit/s).
- 11na : Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11be, 802.11ax et 802.11ac est limitée à la vitesse maximale prise en charge par 802.11na (environ 450 Mbit/s).
- **11a**: Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11ax, 802.11ac et 802.11na est limitée à la vitesse maximale prise en charge par 802.11a (jusqu'à environ 54 Mbit/s).

- 6 GHz
  - 11be : Les clients WiFi 802.11be et 802.11ax peuvent se connecter au point d'accès. Il s'agit de l'option par défaut.
  - 11ax : Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès.

7. Dans le menu **Channel Width** (**largeur du canal**) d'une radio, sélectionnez la largeur du canal, en gardant à l'esprit qu'un canal plus large améliore les performances (aucune interférence ou un minimum d'interférences et de meilleurs débits de données) :
   - 2,4 GHz La largeur du canal dépend du mode sans fil :
     - **11be, 11ac et 11ng**: 20 MHz, 40 MHz ou dynamique 20 / 40 MHz. La valeur par défaut est 20 MHz.
     - (11bg ET 11b) Vous ne pouvez pas sélectionner la largeur du canal.
   - 5 GHz La largeur du canal dépend du mode sans fil :
     - **11be, 11ax et 11ac**: 20 MHz, 40 MHz, 80 MHz, 160 MHz ou dynamique 20 / 40 / 80 / 160 MHz. La valeur par défaut est 40 MHz.
     - 11na : 20 MHz, 40 MHz ou dynamique 20 / 40 MHz. La valeur par défaut est 40 MHz.
     - **11a**: Vous ne pouvez pas sélectionner la largeur du canal.

     Les canaux 40 MHz, 80 MHz et 160 MHz permettent des débits de données plus élevés mais laissent moins de canaux disponibles pour une utilisation sur la radio 5 GHz.
   - 6 GHz La largeur du canal dépend du mode sans fil :

- 11be : 20 MHz, 40 MHz, 80 MHz, 160 MHz, 320 MHz ou dynamique 20 / 40 / 80 / 160 / 320 MHz. La valeur par défaut est 80 MHz.
- 11ax : 20 MHz, 40 MHz, 80 MHz, 160 MHz ou dynamique 20 / 40 / 80 / 160 MHz. La valeur par défaut est 80 MHz.

Pour plus d'informations, consultez la section Permet de changer de canal pour une radio à la page 117.

8. Intervalle de garde L'intervalle de garde protège les transmissions radio contre les interférences. Votre sélection dans le menu **mode sans fil** détermine si vous pouvez définir l'intervalle de garde et, le cas échéant, quels intervalles de garde sont disponibles. Pour les modes WiFi 11a, 11b et 11bg, vous ne pouvez pas définir l'intervalle de garde.

   Dans le menu, sélectionnez l'un des paramètres suivants :

   - **Auto**. L'intervalle de garde est défini automatiquement par le AP. Cette option n'est pas disponible dans les modes WiFi 11be et 11ax.
   - Long-800 ns Cette option est disponible dans les modes 11ax, 11ac, 11na et 11ng. Dans les modes WiFi 11be et 11ax, cette option est le paramètre par défaut.
   - **Double long-1600 ns**: Cette option est disponible uniquement dans les modes WiFi 11be et 11ax.
   - **Quadruple long-3200 ns**: Cette option est disponible uniquement dans les modes WiFi 11be et 11ax
9. Puissance de sortie Dans le menu, sélectionnez la puissance de transmission de la radio. Vous pouvez sélectionner **100%(Max)**, **50%**, **25%**, **12,5 %** ou **4%(min)**. La valeur par défaut est 100 % (Max).

   REMARQUE: Si deux points d'accès ou plus fonctionnent dans la même zone et sur le même canal, des interférences peuvent se produire. Dans ce cas, vous pouvez diminuer la puissance de sortie d'un point d'accès. Assurez-vous que vous respectez les exigences réglementaires concernant la puissance de sortie de la fréquence radio (RF) totale dans votre pays.
10. Canal : Dans le menu, sélectionnez le canal WiFi de la radio. Les canaux et fréquences WiFi disponibles dépendent du pays sélectionné pour le AP et sur la radio. La valeur par défaut est Auto, ce qui permet à la radio de sélectionner automatiquement le canal le plus adapté.

    REMARQUE: Vous n'avez pas besoin de changer le canal WiFi sauf si vous constatez des interférences (indiquées par des pertes de connexion).

REMARQUE: Si vous utilisez plusieurs points d'accès, réduisez les interférences en sélectionnant différents canaux pour les points d'accès adjacents. Nous recommandons un espacement des canaux de quatre canaux sans chevauchement entre les points d'accès adjacents (par exemple, dans la bande 2,4 GHz, utilisez les canaux 1 et 5, ou 6 et 10).

11. Cliquez sur le bouton **Apply** (Appliquer).

    Une fenêtre d'avertissement s'affiche.

12. Cliquez sur le bouton **OK** (Enregistrer).

    La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Permet d'allumer ou d'éteindre une radio

Par défaut, les radios 2,4 GHz, 5 GHz et 6 GHz diffusent. La désactivation d'une radio désactive l'accès WiFi pour la bande associée, ce qui affecte tous les réseaux WiFi (VPN ou SSID) de cette bande. La désactivation d'une radio peut s'avérer utile lors de la configuration, du réglage du réseau ou du dépannage.

Pour activer ou désactiver une radio :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page Wireless Settings (Paramètres Wifi) s'affiche.

5. Effectuez l'une des actions suivantes :

   - **Allumer une radio** : Cochez la case **Activer la radio** pour la radio.
   - **Éteindre une radio** : Décochez la case **ACTIVER la radio** pour la radio.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Permet de modifier le mode préambule d'une radio

Par défaut, tous les types de clients WiFi peuvent accéder à un réseau WiFi sur le point d'accès, c'est-à-dire que les modes WiFi du point d'accès prennent en charge les clients 802.11be, 802.11ax, 802.11ac, 802.11na, 802.11ng, 802.11bg, 802.11b et 802.11a. Vous pouvez modifier les modes WiFi pour limiter l'accès à certains types de clients.

Permet de modifier le mode préambule d'une radio

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page Wireless Settings (Paramètres Wifi) s'affiche.
5. Sélectionnez l'un des boutons radio **mode sans fil** suivants pour une radio, ce qui détermine si vous pouvez définir la largeur de canal et, le cas échéant, quelles sont les largeurs de canal disponibles :

   - 2,4 GHz

  - 11be : Les clients WiFi 802.11be, 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Il s'agit de l'option par défaut.
  - 11ax : Les clients WiFi 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Il s'agit de l'option par défaut.
  - 11 ng Les clients WiFi 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11ax est limitée à la vitesse maximale prise en charge par 802.11ng (environ 450 Mbit/s).
  - 11bg : Les clients WiFi 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11ax et 802.11ng est limitée à la vitesse maximale prise en charge par 802.11bg (environ 54 Mbit/s).
  - 11b : Les clients WiFi 802.11ax, 802.11ng, 802.11bg et 802.11b peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11ax, 802.11n et 802.11bg est limitée à la vitesse maximale prise en charge par 802.11b (environ 11 Mbit/s).
- 5 GHz
  - 11be : Les clients Wi-Fi 802.11be et 802.11ax peuvent se connecter au AP. Il s'agit de l'option par défaut.
  - 11ax : Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès.
  - 11ac : Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11be et 802.11ax est limitée à la vitesse maximale prise en charge par 802.11ac (environ 867 Mbit/s).
  - 11na : Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11be, 802.11ax et 802.11ac est limitée à la vitesse maximale prise en charge par 802.11na (environ 450 Mbit/s).
  - **11a**: Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès. Cependant, la vitesse des clients 802.11ax, 802.11ac et 802.11na est limitée à la vitesse maximale prise en charge par 802.11a (jusqu'à environ 54 Mbit/s).
- 6 GHz
  - 11be : Les clients Wi-Fi 802.11be et 802.11ax peuvent se connecter au AP. Il s'agit de l'option par défaut.
  - 11ax : Les clients WiFi 802.11ax, 802.11ac, 802.11na et 802.11a peuvent se connecter au point d'accès.

6. Cliquez sur le bouton **Apply** (Appliquer).

Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Permet de changer de canal pour une radio

Suivez les directives suivantes lorsque vous déterminez la largeur de canal d'une radio :

- Un canal plus large améliore généralement les performances (aucune interférence ou minimum et meilleurs débits de données).
- Un canal plus étroit entraîne généralement un débit plus faible, mais peut fournir une connexion plus stable dans des situations difficiles, comme un environnement avec une longue distance entre le AP et les clients WiFi et plus d'interférences que la normale.
- La spécification 802.11n permet un canal de 40 MHz en plus du canal hérité de 20 MHz, disponible avec les autres modes.
- Les spécifications 802.11ac et 802.11ax pour la bande 5 GHz (et, par extension, pour la radio 6 GHz) autorisent un canal de 80 MHz et un canal de 160 MHz en plus des canaux de 20 MHz et 40 MHz disponibles avec les autres modes WiFi.
- La spécification 802.11be pour la radio 6 GHz autorise un canal de 320 MHz en plus des largeurs de canal de 20 MHz, 40 MHz, 80 MHz et 160 MHz disponibles avec d'autres modes WiFi.

REMARQUE: Nous vous recommandons de conserver les options par défaut : 20 MHz pour la radio 2,4 GHz, 40 MHz pour la radio 5 GHz et 80 MHz pour la radio 6 GHz.

Le mode WiFi (voir Permet de modifier le mode préambule d'une radio à la page 114) détermine si vous pouvez définir la largeur de canal et, le cas échéant, quelles sont les largeurs de canal disponibles.

Pour changer de canal pour une radio :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l'appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s'affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page Wireless Settings (Paramètres Wifi) s'affiche.

5. Dans le menu **Channel Width** (**largeur du canal**) d'une radio, sélectionnez la largeur du canal, en gardant à l'esprit qu'un canal plus large améliore les performances (aucune interférence ou un minimum d'interférences et de meilleurs débits de données) :

   - 2,4 GHz La largeur du canal dépend du mode sans fil :
     - **11be, 11ax et 11ac**: 20 MHz, 40 MHz ou dynamique 20 / 40 MHz. La valeur par défaut est 20 MHz.
     - (11bg ET 11b) Vous ne pouvez pas sélectionner la largeur du canal.
   - 5 GHz La largeur du canal dépend du mode sans fil :

- **11be, 11ax et 11ac**: 20 MHz, 40 MHz, 80 MHz, 160 MHz ou dynamique 20 / 40 / 80 / 160 MHz. La valeur par défaut est 40 MHz.
- 11na : 20 MHz, 40 MHz ou dynamique 20 / 40 MHz. La valeur par défaut est 40 MHz.
- **11a**: Vous ne pouvez pas sélectionner la largeur du canal.

Les canaux 40 MHz, 80 MHz et 160 MHz permettent des débits de données plus élevés mais laissent moins de canaux disponibles pour une utilisation sur la radio 5 GHz.

- 6 GHz La largeur du canal dépend du mode sans fil :
  - 11be : 20 MHz, 40 MHz, 80 MHz, 160 MHz, 320 MHz ou dynamique 20 / 40 / 80 / 160 / 320 MHz. La valeur par défaut est 80 MHz.
  - 11ax : 20 MHz, 40 MHz, 80 MHz, 160 MHz ou dynamique 20 / 40 / 80 / 160 MHz. La valeur par défaut est 80 MHz.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Modifier l'intervalle de garde d'une radio

Dans le menu, sélectionnez l'intervalle de garde qui protège les transmissions radio contre les interférences. Le mode WiFi (voir Permet de modifier le mode préambule d'une radio à la page 114) détermine si vous pouvez définir l'intervalle de garde et, le cas échéant, quels intervalles de garde sont disponibles. Pour les modes WiFi 11a, 11b et 11bg, vous ne pouvez pas définir l'intervalle de garde.

Respectez les consignes suivantes :

- Un intervalle de garde plus court prend en charge un débit plus élevé dans un environnement dans lequel les périphériques WiFi fonctionnent à une distance plus courte du AP.
- Un intervalle de garde plus long fonctionne bien dans un environnement comportant plusieurs SSID et périphériques WiFi fonctionnant à une plus grande distance du AP.
- Certains périphériques hérités peuvent fonctionner avec un intervalle de garde de –800 ns seulement.

Pour modifier l'intervalle de garde d'une radio :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page Wireless Settings (Paramètres Wifi) s'affiche.

5. Dans le menu **intervalle de garde de** la radio, sélectionnez l'un des paramètres suivants :

   - **Auto**. L'intervalle de garde est défini automatiquement par le AP. Cette option n'est pas disponible dans les modes WiFi 11be et 11ax.
   - Long-800 ns Cette option est disponible dans les modes 11ax, 11ac, 11na et 11ng. Dans les modes WiFi 11be et 11ax, cette option est le paramètre par défaut.
   - **Double long-1600 ns**: Cette option est disponible uniquement dans les modes WiFi 11be et 11ax.
   - **Quadruple long-3200 ns**: Cette option est disponible uniquement dans les modes WiFi 11be et 11ax

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Modifier la puissance de sortie d'une radio

Par défaut, la puissance de sortie du point d'accès est définie au maximum. Si deux points d'accès ou plus fonctionnent dans la même zone et sur le même canal, des interférences peuvent se produire. Dans ce cas, vous pouvez diminuer la puissance de sortie d'un point d'accès. Assurez-vous que vous respectez les exigences réglementaires concernant la puissance de sortie de la fréquence radio (RF) totale dans votre pays.

Pour modifier la puissance de sortie d'une radio :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations,

consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l'appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s'affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page Wireless Settings (Paramètres Wifi) s'affiche.

5. Dans le menu **puissance de sortie de** la radio, sélectionnez **100 % (Max)**, **50 %**, **25 %** , **12,5 %** ou **4 % (min)**.

   La valeur par défaut est 100 % (Max).

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Permet de changer de canal pour une radio

Les canaux et fréquences WiFi disponibles dépendent du pays sélectionné pour le AP et la radio. La valeur par défaut est Auto, ce qui permet à la radio de sélectionner automatiquement le canal le plus adapté.

REMARQUE: Vous n'avez pas besoin de changer le canal WiFi sauf si vous constatez des interférences (indiquées par des pertes de connexion).

REMARQUE: Si vous utilisez plusieurs points d'accès, réduisez les interférences en sélectionnant différents canaux pour les points d'accès adjacents. Nous recommandons un espacement des canaux de quatre canaux sans chevauchement entre les points d'accès adjacents (par exemple, dans la bande 2,4 GHz, utilisez les canaux 1 et 5, ou 6 et 10).

Pour changer de canal pour une radio :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page Wireless Settings (Paramètres Wifi) s'affiche.

5. Dans le menu **canal de** la radio, sélectionnez un canal.

   La valeur par défaut est Auto. Lorsque vous sélectionnez un canal particulier, la sélection de canal devient statique.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Gérer la qualité de service pour une radio WiFi

Vous pouvez spécifier séparément le paramètre de qualité de service (QoS) pour les radios 2,4 GHz, 5 GHz et 6 GHz. Ces paramètres sont activés par défaut pour chaque radio. La désactivation de QoS pour une radio peut affecter le débit et la vitesse du trafic WiFi sur le AP.

Pour gérer les paramètres QoS d'une radio WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page Paramètres QoS s'affiche.
5. Activez ou désactivez les fonctions suivantes pour la radio en sélectionnant les boutons radio **Activer** ou **désactiver** applicables :

   - Wi-Fi Multimedia (WMM) WiFi Multimedia (WMM) est un sous-ensemble de la norme 802.11e. Les informations dépendant du temps, telles que la vidéo ou l'audio, sont prioritaires par rapport au trafic normal. Pour que WMM fonctionne correctement, les clients sans fil doivent également le prendre en charge. En

activant WMM, vous autorisez WMM à contrôler le trafic en amont des périphériques WiFi vers le AP et le trafic en aval du AP vers les périphériques WiFi. WMM définit les quatre files d'attente suivantes par ordre décroissant de priorité :

- **Voice** (Voix). La file d'attente la plus prioritaire avec un délai minimum, ce qui la rend très adaptée aux applications telles que la VoIP et le streaming multimédia.
- Vidéo Deuxième file d'attente prioritaire avec un retard faible. Les applications vidéo sont routées vers cette file d'attente
- **Meilleur effort**: File d'attente de priorité moyenne avec délai moyen. La plupart des applications IP standard utilisent cette file d'attente
- Arrière-plan Arrière-plan : niveau de priorité faible avec haut débit. Les applications non sensibles aux délais, mais nécessitant un haut débit peuvent utiliser cette file d'attente (ex. : FTP)

REMARQUE: Wi-Fi Multimedia (WWM) ne peut pas être désactivé pour les modes 802.11n, 802.11ac, 802.11ax et 802.11be.

- Économie d'énergie WMM L'activation de la fonction d'économie d'énergie WMM permet d'économiser de l'énergie pour les périphériques alimentés par batterie et d'ajuster la consommation d'énergie.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

7

Configurer et gérer un portail captif

Ce chapitre décrit comment configurer et gérer un portail captif sur le AP.

Un portail captif est une page Web que les utilisateurs voient lorsqu'ils tentent de se connecter à un réseau WiFi. Un portail captif inclut une page de démarrage et nécessite généralement une forme d'authentification pour l'utilisateur. Le AP prend en charge deux types de portails captifs :

- **Portail captif accessible par clic** : Portail de base pour lequel la page de démarrage est stockée sur le AP. Pour chaque réseau WiFi, vous pouvez configurer un portail captif à clic unique.
- Portail captif externe Portail hébergé par un fournisseur de portail captif externe. Vous pouvez appliquer un portail captif externe à plusieurs réseaux WiFi ou un portail captif externe unique à chaque réseau WiFi.

Ce chapitre comprend les sections suivantes :

- Configurez un portail captif accessible par clic pour un réseau WiFi
- Configurez un portail captif externe pour un réseau WiFi

REMARQUE: Un portail captif n'est pas compatible avec Multi PSK. Pour activer un portail captif, désactivez d'abord Multi PSK (voir Configurez Multi PSK pour un réseau WiFi à la page 97).

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Configurez un portail captif accessible par clic pour un réseau WiFi

Un portail captif accessible par clic est un portail de base pour lequel la page de démarrage est stockée sur le AP, c'est-à-dire qu'il ne s'agit pas d'un portail captif externe. Utilisez un portail captif accessible par clic pour accueillir ou informer les utilisateurs WiFi et limiter leurs sessions. Vous pouvez demander aux utilisateurs d'accepter un contrat de licence utilisateur final (CLUF) et de les rediriger vers un site Web spécifique. Un portail captif accessible par clic est spécifique au réseau WiFi (SSID) sur lequel vous l'avez configuré.

Pour configurer un portail captif accessible par clic pour un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Cochez la case **Portail captif**.

   La page s'ajuste. Par défaut, le bouton radio **cliquer** est sélectionné.

8. Spécifiez les paramètres de clic comme décrit dans le tableau suivant.

Paramètre	Description
Délai d'expiration de la session (en min)	Entrez le nombre de minutes entre 1 et 1440 après lequel une session WiFi est terminée et un utilisateur doit se reconnecter. La valeur par défaut est 60 minutes.
URL de redirection	Pour rediriger un utilisateur vers un site Web spécifique après la connexion, cochez la case **rediriger l'URL** et saisissez l'URL. Si la case **URL de redirection** est décochée, un utilisateur est dirigé vers la page Web par défaut.
Titre	Saisissez le titre affiché sur la page de connexion au portail captif. Si vous ne personnalisez pas le titre, le titre par défaut s'affiche sur la page de connexion au portail captif.
Message	Saisissez un message à l'intention de l'utilisateur. Ce message s'affiche sur la page de connexion au portail captif. Si vous ne personnalisez pas le message, le message par défaut s'affiche sur la page de connexion au portail captif.

(A continué)

Paramètre	Description
Image JPEG/JPG (max. 500 Ko)	Pour personnaliser l'image affichée sur la page de connexion au portail captif, cliquez sur le bouton **Parcourir** et sélectionnez une image. Si vous ne personnalisez pas l'image, l'image par défaut s'affiche sur la page de connexion au portail captif.
CLUF (max. 1 Ko)	Ce champ inclut un contrat de licence utilisateur final (CLUF) par défaut. Vous pouvez saisir ou copier du texte personnalisé dans le champ. Pour afficher le CLUF sur la page de connexion au portail captif, cochez la case **CLUF**.

9. Pour afficher un aperçu de la page de connexion au portail captif, cliquez sur le bouton **Aperçu**.
10. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés. Les clients WiFi qui tentent de se connecter au SSID s'affichent avec la page de connexion au portail captif.

    REMARQUE: Une session HTTPS est bloquée jusqu'à ce que l'authentification du portail captif se produise.

Configurez un portail captif externe pour un réseau WiFi

Un portail captif externe est un portail hébergé par un fournisseur de portail captif externe. En d'autres termes, ce type de portail n'est pas stocké sur le AP. Pour un portail captif externe, vous devez généralement enregistrer vos appareils auprès du fournisseur et acheter des licences auprès de celui-ci.

Vous pouvez appliquer un portail captif externe à plusieurs réseaux WiFi ou un portail captif externe unique à chaque réseau WiFi

Pour configurer un portail captif externe pour un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Cochez la case **Portail captif**.

   La page s'ajuste. Par défaut, le bouton radio clic est sélectionné.

8. Cliquez sur le bouton radio **Portail captif externe**.

   La page s'ajuste.

9. Dans le champ **URL de la page de démarrage**, entrez l'URL fournie par le fournisseur.

   Cette URL redirige un utilisateur vers la page de démarrage du site Web qui héberge le portail captif. La longueur de l'URL de la page de démarrage peut aller jusqu'à 256 caractères.

10. Sélectionnez l'un des boutons radio **type d'authentification du portail captif** suivants :

- Web/HTTP L'authentification pour l'accès à la page de démarrage s'effectue sur le système AP à l'aide du protocole HTTPS. Spécifiez les paramètres suivants :
  - URL d'authentification Web Saisissez l'URL d'authentification Web fournie par le fournisseur.

    L'URL d'authentification Web peut contenir jusqu'à 256 caractères.
  - Clé : Saisissez les informations d'identification de clé fournies par le fournisseur. Ce champ est facultatif et dépend des exigences d'authentification du fournisseur.

    La longueur de la clé peut aller jusqu'à 32 caractères.
  - Secret Saisissez les informations d'identification secrètes fournies par le fournisseur. Ce champ est facultatif et dépend des exigences d'authentification du fournisseur.

    La longueur de la clé peut aller jusqu'à 64 caractères.
- Radius L'authentification pour l'accès à la page de démarrage se produit sur un serveur d'authentification RADIUS externe (un serveur d'authentification RADIUS secondaire est une option). Le fournisseur peut également avoir besoin d'un serveur RADIUS de comptabilité (un serveur RADIUS de comptabilité secondaire est une option).

  Spécifiez les paramètres suivants pour *chaque* serveur RADIUS, comme indiqué par le fournisseur :
  - Adresse IPv4 : Saisissez l'adresse IP du switch. L'adresse IP est fournie par le fournisseur.
  - **Port**. Entrez le numéro de port utilisé par le serveur. Le numéro de port IP est fourni par le fournisseur. Par défaut, un serveur d'authentification utilise le numéro de port 1812 ; un serveur de comptabilité utilise le numéro de port 1813.

    La plage de numéros de port peut être comprise entre 1 et 65535.
  - Nouveau mot de passe : Saisissez le mot de passe (secret partagé) pour l'interaction avec le serveur. Le mot de passe est fourni par le fournisseur.

    Le mot de passe doit comprendre entre 8 et 64 caractères.
  - **Intervalle comptable** : Entrez l'intervalle de comptabilisation, qui indique le nombre de secondes entre chaque transmission d'une mise à jour provisoire ou d'un paquet actif pour une session spécifique. Le champ intervalle

comptable doit avoir une valeur comprise entre 60 secondes (minimum) et 600 secondes (maximum).

- **NAS-identifier**: Entrez un identifiant de serveur d'accès réseau (NAS-ID).

  Un NAS-ID est utilisé pour distinguer la source d'une demande d'accès ou de comptabilité RADIUS, ce qui permet au serveur RADIUS de choisir une stratégie pour cette demande. Le paramètre NAS-identifier par défaut est l'adresse MAC Ethernet du AP.

11. Sélectionnez l'un des boutons **de sécurité intégrée** suivants pour spécifier si les utilisateurs sont autorisés à accéder à la page de démarrage et à Internet si l'authentification n'est pas possible :
    - Activer. Si l'authentification n'est pas possible, par exemple parce que les serveurs de portail captif ne répondent pas, les utilisateurs sont toujours autorisés à accéder à Internet pendant une période de 30 minutes.
    - Désactiver : Il s'agit de l'option par défaut. Si l'authentification n'est pas possible, les utilisateurs ne peuvent pas accéder à la page de démarrage et ne peuvent pas accéder à Internet. Au lieu de cela, ils reçoivent un message *Oups. Une erreur s'est produite.* Réessayez ultérieurement.
12. Sélectionnez l'un des boutons **autoriser HTTPS** suivants pour spécifier quand le trafic HTTP sécurisé (HTTPS) est autorisé à passer par :
    - Activer. Avant que l'authentification ne se produise, le trafic HTTPS est autorisé à passer par.
    - Désactiver : Il s'agit de l'option par défaut. Le trafic HTTPS est autorisé uniquement *après* authentification.
13. Configurez les paramètres du jardin clos.

    Le jardin clos spécifie les applications externes et les sites auxquels un utilisateur peut accéder à partir du portail captif. Généralement, le fournisseur fournit des informations sur les applications et les sites. La page d'accueil du fournisseur, le nom de domaine et les serveurs d'authentification doivent également être inclus dans le jardin clos. Suivez les directives du fournisseur.

    Vous pouvez faire ce qui suit pour configurer le jardin clos:

    - **Ajouter une seule URL**: Dans le champ de droite, saisissez l'URL, appuyez sur **entrée**, puis cliquez sur le bouton **déplacer** .
    - **Ajouter plusieurs URL**: Dans le champ de droite, collez une liste d'URL, puis cliquez sur le bouton **déplacer**.

- **Supprimer une ou plusieurs URL**: Cochez les cases des URL, puis cliquez sur le bouton **Supprimer**.
- **Supprimer toutes les URL**: Cochez la case **sélectionner tout**, puis cliquez sur le bouton **Supprimer**.

14. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés. Les clients WiFi qui tentent de se connecter au SSID s'affichent avec la page de connexion au portail captif.

8

Gérer l'accès et la sécurité

Ce chapitre décrit comment gérer les fonctions d'accès et de sécurité ainsi que les comptes utilisateur.

Ce chapitre comprend les sections suivantes :

- Gérer les comptes utilisateur
- Bloquer des URL et des mots-clés spécifiques pour l'accès à Internet
- Configurer les serveurs RADIUS
- Gérer la détection des points d'accès voisins
- Gérez les listes de contrôle d'accès MAC globales et les stratégies de trafic
- Gérer l'ordre de priorité du trafic
- Gérez les listes de contrôle d'accès MAC basées sur SSID et les stratégies de trafic pour les réseaux WiFi
- Activer la sécurité L2
- Gérer la protection contre les dénis de service

REMARQUE: Pour plus d'informations sur la sécurité WiFi essentielle (authentification réseau et cryptage), reportez-vous à la section Configurez un réseau WiFi ouvert ou sécurisé à la page 73 ou Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90.

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Gérer les comptes utilisateur

Les comptes d'utilisateur fournissent un accès en lecture/écriture ou en lecture seule à l'interface utilisateur du terminal de AP. Vous ne pouvez pas supprimer le compte d'utilisateur administrateur ou modifier son nom d'utilisateur, mais vous pouvez modifier son mot de passe. Vous pouvez ajouter des comptes pour d'autres utilisateurs, et vous pouvez modifier ou supprimer ces comptes.

Les sections suivantes décrivent comment gérer les comptes utilisateur :

- Ajouter un compte utilisateur
- Modifier le délai d'expiration d'une session utilisateur
- Modifier les paramètres d'un compte utilisateur
- Supprimer un compte utilisateur

Pour plus d'informations sur la modification du mot de passe du compte utilisateur admin par défaut, reportez-vous à la section Modifiez le mot de passe du compte utilisateur admin à la page 246.

Ajouter un compte utilisateur

Pour ajouter un compte utilisateur :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > comptes utilisateur**.
   La page comptes utilisateur s'affiche.
5. Cliquez sur l'icône Ajouter un compte utilisateur.
   Des champs supplémentaires et un menu s'affichent.
6. Spécifiez les paramètres du nouveau compte utilisateur :
   - Nom d'utilisateur : Choisissez un nom d'utilisateur.
     Le nom d'utilisateur doit comporter jusqu'à 15 caractères alphanumériques sans caractères spéciaux. N'utilisez pas admin ou Admin comme nom d'utilisateur.
   - Nouveau mot de passe : Entrez un mot de passe comportant entre 8 et 64 caractères et confirmez-le.
     Le mot de passe doit contenir au moins une lettre majuscule, une lettre minuscule et un chiffre.
   - **Privilège**: Dans le menu, sélectionnez **lecture-écriture** ou **lecture seule**.
   - Expiration de la session ! Utilisez les champs **heures** et **minutes** pour spécifier la période après laquelle une session expire automatiquement et l'utilisateur doit se reconnecter.
     Par défaut, une session expire après 45 minutes.
7. Cliquez sur le bouton **Apply** (Appliquer).
   Les paramètres sont enregistrés.

Modifier le délai d'expiration d'une session utilisateur

Lorsqu'un utilisateur se connecte à l'interface utilisateur du terminal, la session expire automatiquement au bout de 45 minutes. Vous pouvez modifier la période de temporisation, qui s'applique à tous les utilisateurs, y compris l'utilisateur admin.

Pour modifier le délai d'expiration d'une session utilisateur :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > comptes utilisateur** .

La page comptes utilisateur s'affiche.

5. Sous délai de session, utilisez les champs **heures** et **minutes** pour spécifier la période après laquelle une session expire automatiquement et l'utilisateur doit se reconnecter.

   Par défaut, une session expire après 45 minutes.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Votre session est terminée et vous devez vous reconnecter.

Modifier les paramètres d'un compte utilisateur

Vous ne pouvez pas modifier le privilège d'accès pour le compte d'utilisateur admin par défaut.

Pour modifier le nom d'utilisateur, le mot de passe ou le privilège d'accès d'un compte d'utilisateur :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > comptes utilisateur**.
   Les comptes utilisateur existants s'affichent.
5. À droite du compte utilisateur, modifiez les paramètres existants selon vos besoins :
   - Nom d'utilisateur : Saisissez un autre nom d'utilisateur.
     Le nom d'utilisateur doit comporter jusqu'à 15 caractères alphanumériques sans caractères spéciaux. N'utilisez pas admin ou Admin comme nom d'utilisateur.
   - Nouveau mot de passe : Entrez un autre mot de passe de 8 à 64 caractères, puis confirmez-le.
     Le mot de passe doit contenir au moins une lettre majuscule, une lettre minuscule et un chiffre.
   - **Privilège**: Dans le menu, sélectionnez **lecture-écriture** ou **lecture seule**.
6. Cliquez sur le bouton **Apply** (Appliquer).
   Les paramètres sont enregistrés.

Supprimer un compte utilisateur

Vous pouvez supprimer une règle de trafic dont vous n'avez plus besoin. Vous ne pouvez pas supprimer le compte utilisateur admin par défaut.

Pour supprimer un compte utilisateur :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > comptes utilisateur**.

   La page comptes d'utilisateur s'affiche, affichant les comptes d'utilisateur existants.
5. Cliquez sur le **X** à droite du compte utilisateur.

   Une fenêtre d'avertissement s'affiche.
6. Cliquez sur le bouton **Supprimer**.

   La fenêtre contextuelle se ferme et le compte utilisateur est supprimé.

Bloquer des URL et des mots-clés spécifiques pour l'accès à Internet

Vous pouvez définir une liste noire en spécifiant les URL (adresses Web) pour lesquelles l'accès à Internet doit être bloqué. Vous pouvez également spécifier des mots-clés qui amènent le système AP à rejeter les URL contenant ces mots-clés.

Pour créer une liste noire avec des URL et des mots-clés pour lesquels l'accès à Internet doit être bloqué :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > filtrage d'URL** .

   La page filtrage d'URL s'affiche.

5. Sélectionnez le bouton radio Activer.
6. Composez la liste noire des manières suivantes :

   - **URL bloquées** : Pour ajouter une URL à la liste noire, tapez ou copiez l'URL dans le champ supérieur (à gauche du bouton **Ajouter** supérieur) et cliquez sur le bouton **Ajouter** supérieur. Vous pouvez également sélectionner une ou plusieurs URL dans la liste des URL populaires en cochant les cases correspondantes et en cliquant sur le bouton **<< déplacer**.

     Pour supprimer une URL de la liste noire, cochez la case correspondant à l'URL et cliquez sur le bouton **Supprimer** en haut à gauche.

     Lorsque vous bloquez une URL, le domaine et toutes les URL du domaine sont bloqués. Par exemple, si vous ajoutez www.google.com, toutes les pages Web du domaine www.google.com sont bloquées, y compris, par exemple, www.google.com/finance.

   - **Mots-clés bloqués** : Pour ajouter un mot-clé à la liste noire, entrez le mot-clé dans le champ inférieur (à gauche du bouton **Ajouter** inférieur) et cliquez sur le bouton **Ajouter** inférieur.

     Pour supprimer une entrée de mot-clé de la liste noire, cochez la case de l'entrée et cliquez sur le bouton **Supprimer** inférieur.

     Toutes les URL qui contiennent le mot-clé sont bloquées. Par exemple, si vous ajoutez des travaux, toutes les URL contenant des travaux (ou des travaux) sont bloquées.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Configurer les serveurs RADIUS

Si vous utilisez la sécurité WPA2 Enterprise, la sécurité WPA3 Enterprise ou une liste de contrôle d'accès MAC RADIUS, vous devez configurer les serveurs RADIUS pour l'authentification ou pour l'authentification et la comptabilité à l'aide de RADIUS. Vous devez configurer un serveur IPv4 principal et vous pouvez configurer un serveur IPv4 secondaire. Ces paramètres de serveur RADIUS s'appliquent soit à tous les réseaux WiFi qui utilisent la sécurité WPA2 Enterprise ou WPA3 Enterprise (voir Configurez un

réseau WiFi ouvert ou sécurisé à la page 73), soit à tous les réseaux WiFi qui utilisent une liste de contrôle d'accès MAC RADIUS.

REMARQUE: La sécurité WPA2 Enterprise ou la sécurité WPA3 Enterprise et une ACL MAC RADIUS s'excluent mutuellement. Si vous souhaitez utiliser une liste de contrôle d'accès MAC RADIUS pour un réseau WiFi, sélectionnez un autre type de sécurité WiFi (voir Configurez un réseau WiFi ouvert ou sécurisé à la page 73). Si vous souhaitez utiliser la sécurité WPA2 Enterprise ou WPA3 Enterprise pour un réseau WiFi, utilisez une liste de contrôle d'accès MAC locale (voir Gérer les listes de contrôle d'accès MAC pour les clients WiFi à la page 190).

Si vous utilisez une ACL MAC RADIUS, vous devez la définir sur le serveur RADIUS, en utilisant le format de l'exemple suivant pour les adresses MAC des clients dans le serveur RADIUS : Si l'adresse MAC du client est 00:0a:95:9d:68:16, spécifiez-la comme 000a959d6816 dans le serveur RADIUS.

Pour configurer des serveurs RADIUS :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > Paramètres RADIUS** .

   La page Paramètres RADIUS s'affiche.

5. Pour chaque serveur RADIUS à configurer, configurez les paramètres suivants :
   - Adresse IPv4 : Saisissez l'adresse IPv4 du serveur RADIUS. Le AP doit pouvoir accéder à cette adresse IP.
   - **Port**. Entrez le numéro du port UDP sur le système APutilisé pour accéder au serveur RADIUS. Vous pouvez entrer un nombre compris entre 1 et 65535. Le numéro de port par défaut est 1812.
   - Nouveau mot de passe : Saisissez le mot de passe (clé partagée) utilisé entre le système AP et le SERVEUR RADIUS pendant le processus d'authentification ou de comptabilité. La phrase de passe doit comporter entre 8 et 128 caractères. Par défaut, le mot de passe est sharedsecret.
6. Pour activer la comptabilisation sur les serveurs d'authentification, cliquez sur le bouton **Activer la comptabilisation** pour qu'il s'affiche en bleu.
7. Dans le champ **intervalle comptable**, entrez un intervalle comptable.

   Entrez l'intervalle de comptabilisation, qui indique le nombre de secondes entre chaque transmission d'une mise à jour provisoire ou d'un paquet actif pour une session spécifique. Dans le champ intervalle comptable, entrez une valeur comprise entre 60 secondes (minimum) et 600 secondes (maximum).
8. Dans le champ **NAS-identifier**, entrez un identifiant de serveur d'accès réseau (NAS-ID).

   Un NAS-ID est utilisé pour distinguer la source d'une demande d'accès ou de comptabilité RADIUS, ce qui permet au serveur RADIUS de choisir une stratégie

pour cette demande. Le paramètre NAS-identifier par défaut est l'adresse MAC Ethernet du AP.

9. Configurez les paramètres d'authentification suivants, qui s'appliquent à tous les serveurs RADIUS que vous avez configurés :
   - Temps de réauthentification Entrez l'intervalle en secondes après lequel le demandeur (le client WiFi) doit être réauthentifié auprès du serveur RADIUS. Vous pouvez entrer un intervalle compris entre 0 et 99999. L'intervalle par défaut est de 3600 secondes (1 heure). Entrez **0** pour désactiver la réauthentification.
   - **Mettre à jour la clé globale** : Cochez la case pour autoriser la mise à jour de la clé globale et entrez l'intervalle en secondes. Vous pouvez entrer un intervalle compris entre 1 et 99999. Cette case est cochée par défaut et l'intervalle par défaut est de 1800 secondes (30 minutes). Désactivez la case à cocher pour empêcher la mise à jour de la clé globale.
10. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.
11. Pour tester si les serveurs RADIUS configurés peuvent être atteints par le AP, procédez comme suit :
    a. Cliquez sur l'onglet **tester les paramètres RADIUS**.

       La page se développe.
    b. Dans le champ **nom d'utilisateur**, saisissez un nom d'utilisateur qui doit déjà être défini sur le serveur RADIUS et, dans le champ **phrase de passe**, saisissez la phrase de passe associée pour accéder au serveur RADIUS.

       La phrase de passe doit comporter entre 1 et 128 caractères. Tous les caractères spéciaux sont autorisés à l'exception de l'espace.

       La phrase de passe doit comporter entre 1 et 128 caractères. Tous les caractères spéciaux sont autorisés.
    c. Cliquez sur le bouton **DEMARRER LE TEST**.

       Le système AP tente d'atteindre les serveurs RADIUS configurés à l'aide du nom d'utilisateur et de la phrase de passe.

       Les résultats du test s'affichent dans le champ résultat du RAYON DU test.

Gérer la détection des points d'accès voisins

Le AP peut détecter les points d'accès voisins dans une bande radio et vous pouvez les classer comme points d'accès connus.

Si vous activez la détection des points d'accès voisins pour une bande radio, le APscanne régulièrement le réseau WiFi, collecte des informations sur tous les points d'accès sur les canaux et tient à jour une liste des points d'accès détectés dans la zone. Initialement, tous les points d'accès détectés sont affichés dans la liste des points d'accès inconnus. Vous pouvez ajouter des points d'accès que vous connaissez à la liste des points d'accès connus. Vous pouvez également importer une liste de points d'accès connus dans la liste des points d'accès connus.

ATTENTION: Les points d'accès de la liste des points d'accès inconnus nécessitent une enquête plus approfondie. Il peut s'agir de points d'accès indésirables, qui utilisent le SSID d'un réseau légitime. Ces types de points d'accès peuvent représenter une menace sérieuse pour la sécurité.

Les sections suivantes décrivent comment gérer la détection des points d'accès voisins et ajouter des points d'accès voisins à la liste des points d'accès connus :

- Activez la détection des points d'accès voisins et déplacez les points d'accès vers la liste des points d'accès connus
- Importez une liste de points d'accès voisins existante dans la liste des points d'accès connus

REMARQUE: Si vous activez le mode efficacité énergétique, le AP ne peut pas détecter les points d'accès voisins dans les bandes radio 5 GHz et 6 GHz. Pour utiliser la détection des points d'accès voisins dans les bandes radio 5 GHz et 6 GHz, désactivez d'abord le mode efficacité énergétique. Pour plus d'informations, consultez la section Gérer le mode efficacité énergétique à la page 280.

Activez la détection des points d'accès voisins et déplacez les points d'accès vers la liste des points d'accès connus

Le AP peut détecter les points d'accès voisins et vous permet de les classer en tant que points d'accès connus. Une fois que vous avez activé la détection des points d'accès voisins, le système AP conserve une liste des points d'accès qu'il détecte dans la zone. Initialement, tous les points d'accès détectés sont affichés dans la liste des points d'accès inconnus. Vous pouvez déplacer manuellement des points d'accès de la liste des points d'accès inconnus vers la liste des points d'accès connus.

Par défaut, la détection des points d'accès voisins est désactivée.

Pour activer la détection des points d'accès voisins et déplacer les points d'accès détectés vers la liste des points d'accès connus :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > AP voisin** .

   La page qui s'affiche vous permet de sélectionner une bande radio (2,4 GHz, 5 GHz ou 6 GHz).

5. Cliquez sur le bouton **>** à gauche de la bande radio.

   La page AP voisin s'affiche pour la bande radio sélectionnée.

6. Cochez la case **Enable camera AP** (Activer l'OSD de la caméra).

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. La détection des points d'accès voisins est maintenant activée.

8. Pour afficher les points d'accès voisins détectés et les déplacer de la liste des points d'accès inconnus vers la liste des points d'accès connus, procédez comme suit :

   a. Cliquez sur l'onglet **liste des points d'accès inconnus**.

      La page s'ajuste pour afficher les points d'accès inconnus.

   b. Si aucun point d'accès ne s'affiche, cliquez sur le bouton **Actualiser**.

   c. Cochez les cases correspondant aux points d'accès que vous connaissez et auxquels vous faites confiance.

   d. Cliquez sur le bouton **<< déplacer vers la liste des points d'accès connus**.

   e. Cliquez sur l'onglet **liste des points d'accès connus**.

      Les points d'accès sélectionnés s'affichent dans la liste des points d'accès connus.

REMARQUE: Vous pouvez supprimer des points d'accès de la liste des points d'accès connus. Une fois détectés, ces points d'accès s'affichent à nouveau dans la liste des points d'accès inconnus.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Importez une liste de points d'accès voisins existante dans la liste des points d'accès connus

Vous pouvez importer une liste avec les adresses MAC des points d'accès voisins connus dans la liste des points d'accès connus.

Le fichier contenant les adresses MAC doit être au format suivant :

- Les entrées du fichier doivent être des adresses MAC au format hexadécimal, chaque octet étant séparé par un tiret, par exemple 00-11-22-33-44-55.
- Vous devez séparer les entrées par une virgule ou placer les entrées sur des lignes distinctes.
- Le fichier doit être au format texte (c'est-à-dire avec une extension `.txt` ou).

Pour plus d'informations sur l'activation de la détection des points d'accès voisins, reportez-vous à la section Activez la détection des points d'accès voisins et déplacez les points d'accès vers la liste des points d'accès connus à la page 148.

Pour importer une liste avec les adresses MAC des points d'accès voisins connus dans la liste des points d'accès connus :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

Vous gérez le AP via :

- **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

  REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > AP voisin** .

   La page qui s'affiche vous permet de sélectionner la bande radio (2,4 GHz, 5 GHz ou 6 GHz).

5. Cliquez sur le bouton **>** à gauche de la bande radio.

   La page AP voisin s'affiche pour la bande radio sélectionnée.

6. Pour télécharger un échantillon d'une liste de points d'accès au format requis pour l'importation dans la liste de points d'accès connus, cliquez sur le lien **Télécharger un échantillon**.

7. Importez et composez la liste des points d'accès connus de la manière suivante :

   a. Remplacez ou fusionnez les adresses MAC de la liste d'importation avec les adresses MAC de la liste des points d'accès connus en sélectionnant l'un des boutons radio suivants :

      - Remplacer Les adresses MAC de la liste des points d'accès connus sont remplacées par celles de la liste d'importation.
      - **Fusionner**: Les adresses MAC de la liste des points d'accès connus sont fusionnées avec celles de la liste d'importation.

   b. Cliquez sur le bouton **Parcourir** et naviguez jusqu'au fichier d'importation et sélectionnez-le.

Les adresses MAC de la liste d'importation sont placées dans la liste des points d'accès connus.

c. Pour supprimer une adresse MAC de la liste des points d'accès connus, sélectionnez l'adresse MAC et cliquez sur le bouton **Supprimer**.

   Lorsque vous supprimez un appareil de la liste des points d'accès connus, une fois que le AP détecte à nouveau l'appareil, il est placé à nouveau dans la liste des points d'accès connus.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérez les listes de contrôle d'accès MAC globales et les stratégies de trafic

Les listes de contrôle d'accès MAC globales vous permettent de contrôler le trafic de diffusion et de multidiffusion à partir du LAN câblé ; les stratégies de trafic globales vous permettent de contrôler le trafic entrant à partir du LAN câblé, le trafic sortant vers le LAN câblé et le trafic entre les différents points d'accès virtuels sur le AP. (Un PAV est un point d'accès virtuel qui diffuse sur le même SSID et la même radio.)

Le système AP applique ces listes de contrôle d'accès MAC globales et ces stratégies de trafic dans l'ordre de priorité suivant :

1. **Trafic broadcast et multicast** : Autorise le trafic de diffusion et de multidiffusion entrant à partir de tous les périphériques du réseau local filaire ou uniquement à partir de périphériques spécifiques du réseau local filaire. Le trafic entrant provenant du réseau local filaire peut provenir d'un routeur connecté, d'un commutateur, d'un client filaire, etc.

   Pour plus d'informations, consultez la section Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé à la page 154.

2. Filtre antibruit sans fil Permet d'activer et de modifier huit règles de trafic génériques pour le trafic DHCP entrant et sortant, ARP, IPv6, de diffusion et de multidiffusion spécifique. Ces huit règles sont préconfigurées, mais pas activées par défaut.

Pour en savoir plus, consultez les sections Activez ou désactivez le filtre antibruit sans fil à la page 160 et Activez, désactivez ou modifiez une règle de trafic dans le filtre antibruit sans fil à la page 161.

3. Filtre de trafic global Permet d'ajouter et d'activer des règles de trafic personnalisées qui autorisent ou refusent le trafic en fonction de la couche réseau (adresses MAC ou adresses IP) et d'un protocole sélectionné. Ce trafic peut être entrant, sortant ou dans les deux sens.

   Pour plus d'informations, consultez la section Gérer le filtre de trafic global à la page 167.

Ces listes de contrôle d'accès MAC globales et ces stratégies de trafic s'appliquent à tous les réseaux WiFi (SSID). Vous pouvez également gérer les listes de contrôle d'accès MAC et les stratégies de trafic que vous pouvez appliquer à des SSID individuels (voir Gérez les listes de contrôle d'accès MAC basées sur SSID et les stratégies de trafic pour les réseaux WiFi à la page 189).

Listes de contrôle d'accès MAC globales pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé

Par défaut, tout périphérique est autorisé à envoyer du trafic de diffusion et de multidiffusion du réseau local câblé au AP.

Toutefois, vous pouvez configurer une liste de contrôle d'accès (ACL) basée sur un maximum de 256 adresses MAC pour les périphériques autorisés à envoyer du trafic de diffusion et de multidiffusion à partir du réseau local câblé. Le trafic de diffusion et de multidiffusion provenant des périphériques du réseau local câblé qui ne figurent pas sur cette liste de contrôle d'accès est rejeté par AP.
La liste de contrôle d'accès fonctionne comme suit :

- Un périphérique pour lequel vous placez l'adresse MAC dans la liste de contrôle d'accès est autorisé à envoyer du trafic de diffusion et de multidiffusion du LAN vers n'importe quel réseau WiFi sur le AP.
- Le trafic de diffusion et de multidiffusion provenant de tous les autres périphériques du réseau local est rejeté par AP.

La liste de contrôle d'accès ne prend effet qu'une fois que vous l'avez activée.

Les sections suivantes décrivent comment vous pouvez gérer les listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir de périphériques sur le réseau local filaire :

- Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé
- Importez une ACL MAC existante pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé
- Bloquez tout le trafic de diffusion et de multidiffusion à partir du réseau local filaire

Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé

Par défaut, le trafic de diffusion et de multidiffusion provenant de n'importe quel périphérique sur le réseau local filaire peut atteindre les réseaux WiFi sur le AP.

Vous pouvez composer une seule liste de contrôle d'accès MAC (ACL) pour autoriser le trafic de diffusion et de multidiffusion uniquement à partir de périphériques spécifiques sur le réseau local câblé. Lorsque vous activez cette liste de contrôle d'accès, le trafic de diffusion et de multidiffusion provenant des terminaux sur la liste de contrôle d'accès est autorisé à atteindre les réseaux WiFi sur le AP. Le trafic de diffusion et de multidiffusion provenant d'autres périphériques sur le réseau local câblé est rejeté par AP. La liste de contrôle d'accès peut contenir jusqu'à 256 adresses MAC. Si elle est activée, cette liste de contrôle d'accès s'applique à *tous les* réseaux WiFi sur le AP.

Par défaut, cette ACL MAC est désactivée et n'inclut aucune station. Vous pouvez ajouter manuellement des périphériques, importer des périphériques (voir Importez une ACL MAC existante pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé à la page 156) ou effectuer les deux.

Pour configurer manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir du réseau local filaire :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

Vous gérez le AP via :

- **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

  REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> Allow Broadcast/Multicast Traffic – LAN**.
   La page s'ajuste.
   Par défaut, la case autoriser le trafic de diffusion/multidiffusion - LAN est cochée et le bouton radio autoriser tous les périphériques est sélectionné.
6. Sélectionnez le bouton radio **autoriser le trafic uniquement à partir de périphériques spécifiés**.
   La page s'ajuste.
7. Composez la liste de contrôle d'accès de la manière suivante :
   - Pour ajouter manuellement un périphérique au tableau stations autorisées, entrez l'adresse MAC au format 00-00-00-00-00-00 dans le tableau de droite, puis cliquez sur le bouton **<< déplacer**.
     Le périphérique est ajouté au tableau stations autorisées. Vous pouvez ajouter plusieurs périphériques simultanément.
   - Pour supprimer un périphérique du tableau stations autorisées, cochez la case correspondante, puis cliquez sur le bouton **Supprimer**.

Vous pouvez effectuer une recherche dans le tableau stations disponibles.

- Pour supprimer tous les périphériques du tableau stations autorisées afin de pouvoir recomposer la liste de contrôle d'accès, cochez la case **sélectionner tout**, puis cliquez sur le bouton **Supprimer**.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

   Le trafic haut débit et multicast provenant des périphériques du tableau stations autorisées est autorisé à atteindre les réseaux WiFi sur le AP.

Importez une ACL MAC existante pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé

Vous pouvez importer une liste de contrôle d'accès (ACL) existante basée sur un maximum de 256 adresses MAC. Vous pouvez importer la liste dans n'importe quelle liste de contrôle d'accès MAC, mais les adresses MAC de la liste ne sont disponibles que pour la liste de contrôle d'accès MAC dans laquelle vous importez la liste. Autrement dit, si vous souhaitez utiliser la même liste dans un autre (type de) ACL MAC, vous devez également importer la liste dans cette ACL MAC.

Le fichier contenant les adresses MAC doit être au format suivant :

- Les entrées du fichier doivent être des adresses MAC au format hexadécimal, chaque octet étant séparé par un tiret, par exemple 00-11-22-33-44-55.
- Vous devez séparer les entrées par une virgule ou placer les entrées sur des lignes distinctes.
- Le fichier doit être au format texte (c'est-à-dire avec une extension `.txt` ou).

Vous pouvez utiliser la liste de contrôle d'accès MAC pour autoriser le trafic de diffusion et de multidiffusion uniquement à partir de périphériques spécifiques sur le réseau local filaire. Si elle est activée, cette liste de contrôle d'accès s'applique à *tous les* réseaux WiFi sur le AP.

Pour importer une ACL MAC existante pour le trafic de diffusion et de multidiffusion à partir du réseau local filaire :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.

   La page Traffic Policies s'affiche.

5. Cliquez sur l'onglet **> Allow Broadcast/Multicast Traffic – LAN**.

   La page s'ajuste.

   Par défaut, la case autoriser le trafic de diffusion/multidiffusion - LAN est cochée et le bouton radio autoriser tous les périphériques est sélectionné.

6. Sélectionnez le bouton radio **autoriser le trafic uniquement à partir de périphériques spécifiés**.

   La page s'ajuste.

7. Pour télécharger un exemple d'ACL MAC au format requis pour l'importation, cliquez sur le lien **Télécharger un exemple**.

8. Importez et composez l'ACL de la manière suivante :

   a. Remplacez ou fusionnez les adresses MAC de la liste d'importation avec les adresses MAC du tableau stations autorisées (si elles figurent déjà dans le tableau) en sélectionnant l'un des boutons radio suivants :

- Remplacer Les adresses MAC de la table stations autorisées sont remplacées par celles de la liste d'importation.
- **Fusionner**: Les adresses MAC de la table stations autorisées sont fusionnées avec celles de la liste d'importation.

b. Cliquez sur le bouton **Parcourir** et naviguez jusqu'au fichier d'importation et sélectionnez-le.

Les adresses MAC de la liste d'importation sont placées dans le tableau stations autorisées.

c. Pour supprimer une adresse MAC du tableau stations autorisées, sélectionnez l'adresse MAC et cliquez sur le bouton **Supprimer**.

Vous pouvez effectuer une recherche dans le tableau stations autorisées.

9. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Pour plus d'informations sur l'ajout manuel d'adresses MAC à celles du tableau stations autorisées, reportez-vous à la section Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé à la page 154.

Le trafic haut débit et multicast provenant des périphériques du tableau stations autorisées est autorisé à atteindre les réseaux WiFi sur le AP.

Bloquez tout le trafic de diffusion et de multidiffusion à partir du réseau local filaire

Par défaut, le trafic de diffusion et de multidiffusion provenant de n'importe quel périphérique sur le réseau local filaire peut atteindre les réseaux WiFi sur le AP. Vous pouvez bloquer tout le trafic de diffusion et de multidiffusion du réseau local filaire, empêchant ainsi ce type de trafic d'atteindre les réseaux WiFi sur le AP.

Pour bloquer tout le trafic de diffusion et de multidiffusion à partir du réseau local filaire :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.

   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> Allow Broadcast/Multicast Traffic – LAN**.

   La page s'ajuste.
6. Désactivez le bouton radio **autoriser le trafic de diffusion/multidiffusion - LAN**.
7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

   Le trafic haut débit et multicast du réseau local câblé n'est pas autorisé à atteindre les réseaux WiFi sur le AP.

Gérer le filtre antibruit sans fil

Par défaut, aucune restriction n'existe pour le trafic DHCP, ARP, IPv6, broadcast et multicast pour tout port, adresse IP ou direction du trafic.

Le AP fournit huit stratégies de trafic préconfigurées (c'est-à-dire des règles de trafic) qui peuvent empêcher le trafic générique d'envahir les réseaux WiFi. Ces règles sont appelées filtre antibruit sans fil et sont désactivées par défaut. Vous pouvez activer le filtre antibruit sans fil, puis activer ou désactiver des règles de trafic individuelles.

La liste de contrôle d'accès MAC qui contrôle le trafic de diffusion et de multidiffusion entrant a priorité sur les stratégies de trafic dans le filtre antibruit sans fil.

Les sections suivantes décrivent comment gérer le filtre antibruit sans fil :

- Activez ou désactivez le filtre antibruit sans fil
- Activez, désactivez ou modifiez une règle de trafic dans le filtre antibruit sans fil
- Modifiez la priorité d'une règle de trafic dans le profil application QoS

Activez ou désactivez le filtre antibruit sans fil

Par défaut, le filtre antibruit sans fil est désactivé, de même que toutes les règles de trafic individuelles du filtre antibruit sans fil. Une règle ne peut devenir active qu'après avoir activé le filtre antibruit sans fil et la règle (voir Activez, désactivez ou modifiez une règle de trafic dans le filtre antibruit sans fil à la page 161).

Vous ne pouvez pas ajouter ou supprimer une règle de trafic dans le filtre de bruit sans fil, mais vous pouvez modifier chaque règle de trafic pour l'adapter à votre situation réseau spécifique.

Pour activer ou désactiver le filtre antibruit sans fil :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> filtres de trafic MAC/IP**.
   La page s'ajuste.
6. Cliquez sur l'onglet **> filtre antibruit sans fil**.
   Le tableau des règles de circulation s'affiche.
7. Activez ou désactivez la case à cocher **Activer le filtre antibruit sans fil** :
   - cochée. Le filtre antibruit sans fil est activé.
   - **Case décochée**: Le filtre antibruit sans fil est désactivé.
8. Cliquez sur le bouton **Apply** (Appliquer).
   Les paramètres sont enregistrés.

Activez, désactivez ou modifiez une règle de trafic dans le filtre antibruit sans fil

Vous ne pouvez pas ajouter ou supprimer une stratégie de trafic (c'est-à-dire une règle de trafic) du filtre antibruit sans fil, mais vous pouvez modifier chaque règle de trafic pour l'adapter à votre situation réseau spécifique. Vous pouvez également activer ou désactiver des règles de trafic individuelles.

ATTENTION: Outre l'activation ou la désactivation des règles de trafic dans le filtre antibruit sans fil, nous vous recommandons de modifier les paramètres des règles de trafic uniquement si vous en comprenez parfaitement les conséquences. Une configuration incorrecte peut entraîner des problèmes de connectivité pour tous les périphériques connectés ou tentant de se connecter à AP.

Pour activer, désactiver ou modifier une règle de trafic individuelle dans le filtre antibruit sans fil :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l'appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s'affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> filtres de trafic MAC/IP**.
   La page s'ajuste.
6. Cliquez sur l'onglet **> filtre antibruit sans fil**.
   Le tableau des règles de circulation s'affiche. Par défaut, toutes les règles de trafic sont désactivées.
7. Si le filtre antibruit sans fil est désactivé, cochez la case **Activer le filtre antibruit sans fil**.
8. Cochez la case d'une règle de trafic, puis cliquez sur l'icône **en forme de crayon**.
   La fenêtre contextuelle Ajouter/modifier une règle s'affiche.
9. Réglez les paramètres suivants en fonction de vos besoins :

   REMARQUE: Vous pouvez activer ou désactiver la règle DROP IPv6 Traffic, mais vous ne pouvez pas la modifier.

   - Nom de la règle Vous pouvez modifier le nom de réseau par défaut. Ce qui suit s'applique au nom :
     - doit être un nom alphanumérique unique
     - peut contenir jusqu'à 32 caractères
     - ne peut inclure que les caractères spéciaux ', '-' et '_'
     - Doit commencer et se terminer par un caractère alphanumérique.
   - Etat : Sélectionnez un bouton radio :
     - Activer. Une fois que vous avez cliqué sur le bouton appliquer, la règle prend effet si le filtre antibruit sans fil est activé.
     - Désactiver : Vous pouvez modifier la règle, mais une fois que vous avez cliqué sur le bouton appliquer, la règle prise ne prend pas effet, même si le filtre antibruit sans fil est activé. Par défaut, une règle est désactivée.
   - Action : Sélectionnez un bouton radio :
     - **Autoriser**. Le trafic qui correspond à la règle est autorisé à passer par le réseau WiFi.
     - Refuser Le trafic correspondant à la règle est abandonné.
   - Direction Sélectionnez un bouton radio :

- po. La règle de trafic s'applique uniquement au trafic entrant à partir d'un réseau WiFi.
- **Sortie**: La règle de trafic s'applique uniquement au trafic sortant vers un réseau WiFi.
- **Les deux**: La règle de trafic s'applique à la fois au trafic entrant à partir d'un réseau WiFi et au trafic sortant à destination d'un réseau WiFi.

- **Couche réseau** : Sélectionnez un bouton radio :
  - MAC : La règle de trafic filtre les paquets au niveau MAC.
  - IP : La règle de trafic filtre les paquets au niveau IP.
- **Protocol** (Protocole). Dans le menu Protocole, sélectionnez le protocole.
  - **Tout**: La règle de circulation s'applique à tout trafic.
  - ARP La règle de trafic s'applique uniquement au trafic ARP (Address Resolution Protocol).
  - **TCP**. La règle de trafic s'applique uniquement au trafic TCP (transmission Control Protocol).
  - **UDP**. La règle de trafic s'applique uniquement au trafic UDP (User Datagram Protocol).
  - **ICMP**: La règle de trafic s'applique uniquement au trafic ICMP (Internet Control message Protocol).
  - IGMP La règle de trafic s'applique uniquement au trafic ICMP (Internet Group Management Protocol).
- **Source**. Pour définir la source du trafic auquel la règle de trafic doit s'appliquer, procédez comme suit :
  a. Dans le menu **type**, sélectionnez le type d'adresse MAC ou IP source, en fonction de la couche réseau (MAC ou IP) sélectionnée :
     - **Tout**: La règle de trafic est appliquée à toute adresse MAC ou IP source.
     - **Adresse MAC** (niveau MAC uniquement) : La règle de trafic s'applique uniquement à l'adresse MAC source que vous spécifiez dans le champ **adresse MAC**.

- **Adresse IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement à l'adresse IP source que vous spécifiez dans le champ **adresse IP**.
- **Sous-réseau IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement au sous-réseau IP source que vous spécifiez dans les champs **adresse réseau** et **masque réseau**.

  La longueur du masque réseau doit être comprise entre 8 et 32 chiffres.

b. Dans le champ **Port**, saisissez un numéro de port source auquel la règle de trafic doit s'appliquer.

   Le numéro de port doit être compris entre 1 et 65535.

- Destination Pour définir la destination du trafic auquel la règle de trafic doit s'appliquer, procédez comme suit :

  a. Dans le menu **type**, sélectionnez le type d'adresse MAC ou IP de destination, en fonction de la couche réseau (MAC ou IP) sélectionnée :

  - **Tout**: La règle de trafic est appliquée à toute adresse MAC ou IP de destination.
  - **Adresse MAC** (niveau MAC uniquement) : La règle de trafic s'applique uniquement à l'adresse MAC de destination que vous spécifiez dans le champ **adresse MAC**.
  - **Adresse IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement à l'adresse IP de destination que vous spécifiez dans le champ **adresse IP**.
  - **Sous-réseau IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement au sous-réseau IP de destination que vous spécifiez dans les champs **adresse réseau** et **masque réseau**.

    La longueur du masque réseau doit être comprise entre 8 et 32 chiffres.

  b. Dans le champ **Port**, saisissez un numéro de port de destination auquel la règle de trafic doit s'appliquer.

     Le numéro de port doit être compris entre 1 et 65535.

10. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK**.

    La page filtre de bruit sans fil s'affiche à nouveau.

11. Pour modifier la priorité de la règle de trafic, pointez sur l'icône **à six points** à gauche de la règle de trafic, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.
12. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

Modifiez la priorité d'une règle de trafic dans le profil application QoS

Vous pouvez modifier la priorité d'une règle de trafic dans le profil application QoS.

Pour modifier la priorité d'une règle de trafic individuelle dans le profil application QoS :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.

   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> priorité du trafic**.

   La page s'ajuste.
6. Cliquez sur l'onglet **> application QoS**.

   Le tableau des règles de circulation s'affiche.
7. Si le profil application QoS est désactivé, cochez la case **Activer application QoS**.
8. Pointez sur l'icône **à six points** à gauche de la règle de trafic dont vous souhaitez modifier la priorité, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.
9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérer le filtre de trafic global

Le filtre de trafic global vous permet d'ajouter des stratégies de trafic personnalisées que vous pouvez appliquer globalement au trafic entrant et sortant pour tous les réseaux WiFi.

La liste de contrôle d'accès MAC qui contrôle le trafic de diffusion et de multidiffusion entrant et les stratégies de trafic dans le filtre antibruit sans fil ont priorité sur les stratégies de trafic que vous ajoutez au filtre de trafic global.

Les sections suivantes décrivent comment gérer le filtre de trafic global :

- Activez ou désactivez le filtre de trafic global
- Ajoutez une règle de trafic au filtre de trafic global
- Modifiez une règle de trafic dans le filtre de trafic global
- Modifiez la priorité d'une règle de trafic dans le filtre de trafic global
- Supprimez une règle de trafic du filtre de trafic global

Activez ou désactivez le filtre de trafic global

Par défaut, le filtre de trafic global ne contient aucune stratégie de trafic (c'est-à-dire, des règles de trafic). Vous pouvez ajouter une règle (voir Ajoutez une règle de trafic au filtre de trafic global à la page 169), modifier une règle existante et supprimer une règle dont vous n'avez plus besoin.

La désactivation du filtre de trafic global ne supprime pas les règles de trafic que vous avez ajoutées au filtre de trafic global.

Pour activer ou désactiver le filtre de trafic global :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> filtres de trafic MAC/IP**.
   La page s'ajuste.
6. Cliquez sur l'onglet **> filtre de trafic global**.
   Le tableau des règles de circulation s'affiche. Si vous n'avez pas encore ajouté de règles, la table est vide.
7. Activez ou désactivez la case à cocher **Activer le filtre de trafic global** :
   - cochée. Le filtre de trafic global est activé.
   - **Case décochée**: Le filtre de trafic global est désactivé.
8. Cliquez sur le bouton **Apply** (Appliquer).
   Les paramètres sont enregistrés.

Ajoutez une règle de trafic au filtre de trafic global

Vous pouvez ajouter jusqu'à 16 stratégies de trafic (c'est-à-dire des règles de trafic) au filtre de trafic global. La priorité des règles de trafic est attribuée dans l'ordre dans lequel vous ajoutez les règles. Autrement dit, la première règle que vous ajoutez se voit attribuer la première priorité (la plus élevée), la deuxième règle se voit attribuer la deuxième priorité, et ainsi de suite. Toutefois, vous pouvez modifier la priorité.

⚠ **ATTENTION:** Nous vous recommandons d'ajouter des règles de trafic globales uniquement si vous en comprenez parfaitement les conséquences. Une configuration incorrecte peut entraîner des problèmes de connectivité pour tous les périphériques connectés ou tentant de se connecter à AP.

Pour ajouter une règle de trafic au filtre de trafic global :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.
   La page de connexion s'affiche.
   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l'appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s'affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> filtres de trafic MAC/IP**.

   La page s'ajuste.
6. Cliquez sur l'onglet **> filtre de trafic global**.
   Le tableau des règles de circulation s'affiche. Si vous n'avez pas encore ajouté de règles, la table est vide.
7. Cliquez sur l'icône **plus**.

   La fenêtre contextuelle Ajouter/modifier une règle s'affiche.
8. Réglez les paramètres suivants en fonction de vos besoins :
   - Nom de la règle Vous pouvez modifier le nom de réseau par défaut. Ce qui suit s'applique au nom :
     - doit être un nom alphanumérique unique
     - peut contenir jusqu'à 32 caractères

  - ne peut inclure que les caractères spéciaux ', '-' et '_'
  - Doit commencer et se terminer par un caractère alphanumérique.
- Etat : Sélectionnez un bouton radio :
  - Activer. Après avoir cliqué sur le bouton appliquer, la règle prend effet si le filtre de trafic global est activé.
  - Désactiver : Vous pouvez modifier la règle, mais une fois que vous avez cliqué sur le bouton appliquer, la règle prise ne prend pas effet, même si le filtre de trafic global est activé. Par défaut, une règle est désactivée.
- Action : Sélectionnez un bouton radio :
  - **Autoriser**. Le trafic qui correspond à la règle est autorisé à passer par le réseau WiFi.
  - Refuser Le trafic correspondant à la règle est abandonné.
- Direction Sélectionnez un bouton radio :
  - po. La règle de trafic s'applique uniquement au trafic entrant à partir d'un réseau WiFi.
  - **Sortie**: Les règles de trafic s'appliquent uniquement au trafic sortant vers un réseau WiFi.
  - **Les deux**: La règle de trafic s'applique à la fois au trafic entrant à partir d'un réseau WiFi et au trafic sortant à destination d'un réseau WiFi.
- **Couche réseau** : Sélectionnez un bouton radio :
  - MAC : La règle de trafic filtre les paquets au niveau MAC.
  - IP : La règle de trafic filtre les paquets au niveau IP.
- **Protocol** (Protocole). Dans le menu Protocole, sélectionnez le protocole.
  - **Tout**: La règle de circulation s'applique à tout trafic.
  - ARP La règle de trafic s'applique uniquement au trafic ARP (Address Resolution Protocol).
  - **TCP**. La règle de trafic s'applique uniquement au trafic TCP (transmission Control Protocol).
  - **UDP**. La règle de trafic s'applique uniquement au trafic UDP (User Datagram Protocol).
  - **ICMP**: La règle de trafic s'applique uniquement au trafic ICMP (Internet Control message Protocol).
  - IGMP La règle de trafic s'applique uniquement au trafic ICMP (Internet Group Management Protocol).

- **Source**. Pour définir la source du trafic auquel la règle de trafic doit s'appliquer, procédez comme suit :
  a. Dans le menu **type**, sélectionnez le type d'adresse MAC ou IP source, en fonction de la couche réseau (MAC ou IP) sélectionnée :
     - **Tout**: La règle de trafic est appliquée à toute adresse MAC ou IP source.
     - **Adresse MAC** (niveau MAC uniquement) : La règle de trafic s'applique uniquement à l'adresse MAC source que vous spécifiez dans le champ **adresse MAC**.
     - **Adresse IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement à l'adresse IP source que vous spécifiez dans le champ **adresse IP**.
     - **Sous-réseau IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement au sous-réseau IP source que vous spécifiez dans les champs **adresse réseau** et **masque réseau**.

       La longueur du masque réseau doit être comprise entre 8 et 32 chiffres.
  b. Dans le champ **Port**, saisissez un numéro de port source auquel la règle de trafic doit s'appliquer.

     Le numéro de port doit être compris entre 1 et 65535.
- Destination Pour définir la destination du trafic auquel la règle de trafic doit s'appliquer, procédez comme suit :
  a. Dans le menu **type**, sélectionnez le type d'adresse MAC ou IP de destination, en fonction de la couche réseau (MAC ou IP) sélectionnée :
     - **Tout**: La règle de trafic est appliquée à toute adresse MAC ou IP de destination.
     - **Adresse MAC** (niveau MAC uniquement) : La règle de trafic s'applique uniquement à l'adresse MAC de destination que vous spécifiez dans le champ **adresse MAC**.
     - **Adresse IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement à l'adresse IP de destination que vous spécifiez dans le champ **adresse IP**.
     - **Sous-réseau IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement au sous-réseau IP de destination que vous spécifiez dans les champs **adresse réseau** et **masque réseau**.

La longueur du masque réseau doit être comprise entre 8 et 32 chiffres.

b. Dans le champ **Port**, saisissez un numéro de port de destination auquel la règle de trafic doit s'appliquer.

Le numéro de port doit être compris entre 1 et 65535.

9. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK**.

La page filtre de trafic global s'affiche à nouveau.

10. Pour modifier la priorité de la règle de trafic, pointez sur l'icône **à six points** à gauche de la règle de trafic, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.

Le numéro de priorité s'ajuste.

11. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Modifiez une règle de trafic dans le filtre de trafic global

Vous pouvez modifier une règle de trafic existante dans le filtre de trafic global.

Pour modifier une règle de trafic existante dans le filtre de trafic global :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> filtres de trafic MAC/IP**.
   La page s'ajuste.
6. Cliquez sur l'onglet **> filtre de trafic global**.
   Le tableau des règles de circulation s'affiche.
7. Si le filtre de trafic global est désactivé, cochez la case **Activer le filtre de trafic global**.
8. Cochez la case de la règle de trafic, puis cliquez sur l'icône **en forme de crayon**.
   La fenêtre contextuelle Ajouter/modifier une règle de trafic s'affiche.
9. Modifiez les paramètres en fonction de vos besoins.
   Pour plus d'informations sur les paramètres, reportez-vous à la section Ajoutez une règle de trafic au filtre de trafic global à la page 169.
10. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK**.
    La page filtre de trafic global s'affiche à nouveau.
11. Pour modifier la priorité de la règle de trafic, pointez sur l'icône **à six points** à gauche de la règle de trafic, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.

Le numéro de priorité s'ajuste.

12. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

Modifiez la priorité d'une règle de trafic dans le filtre de trafic global

Vous pouvez modifier la priorité d'une règle de trafic existante dans le filtre de trafic global.

Pour modifier la priorité d'une règle de trafic existante dans le filtre de trafic global :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> filtres de trafic MAC/IP**.
   La page s'ajuste.
6. Cliquez sur l'onglet **> filtre de trafic global**.
   Le tableau des règles de circulation s'affiche.
7. Si le filtre de trafic global est désactivé, cochez la case **Activer le filtre de trafic global**.
8. Pointez sur l'icône **à six points** à gauche de la règle de trafic dont vous souhaitez modifier la priorité, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.
   Le numéro de priorité s'ajuste.
9. Cliquez sur le bouton **Apply** (Appliquer).
   Les paramètres sont enregistrés.

Supprimez une règle de trafic du filtre de trafic global

Vous pouvez supprimer une règle de trafic dont vous n'avez plus besoin.

Pour supprimer une règle de trafic du filtre de trafic global :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.
   La page de connexion s'affiche.
   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.
   Vous gérez le AP via :

- **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

  REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> filtres de trafic MAC/IP**.
   La page s'ajuste.
6. Cliquez sur l'onglet **> filtre de trafic global**.
   Le tableau des règles de circulation s'affiche.
7. Si le filtre de trafic global est désactivé, cochez la case **Activer le filtre de trafic global**.
8. Cochez la case de la règle de trafic, puis cliquez sur l'icône de **la corbeille**.
   La règle de trafic est supprimée.
9. Cliquez sur le bouton **Apply** (Appliquer).
   Les paramètres sont enregistrés.

Gérer l'ordre de priorité du trafic

Vous pouvez utiliser la hiérarchisation du trafic pour hiérarchiser le trafic entrant ou sortant du point d'accès en fonction de l'adresse IP, du numéro de port ou des

protocoles. Pour hiérarchiser le trafic, vous pouvez configurer des règles qui correspondent au trafic. Vous pouvez également filtrer la priorité du trafic en fonction du réseau, de la voix, de la vidéo, de l'arrière-plan et du meilleur effort.

REMARQUE: Assurez-vous de configurer les règles correctement. Si vous configurez des règles de manière incorrecte, elles peuvent perturber les réseaux WiFi.

Il existe deux profils disponibles qui s'appliquent au trafic sur tous les SSID sur le AP:

- **Application QoS** : Pour plus d'informations, consultez la section Gérer le profil de trafic application QoS à la page 178.
- **Règle globale** : Pour plus d'informations, consultez la section Gérer le profil de règle globale à la page 183.

Gérer le profil de trafic application QoS

Le profil de trafic application QoS est constitué d'un ensemble de six règles prédéfinies. Ces règles hiérarchisent le trafic pour certaines applications ou protocoles courants. Vous ne pouvez pas ajouter ou supprimer une règle prédéfinie, mais vous pouvez modifier les numéros de port et l'état. Par défaut, une règle est désactivée, mais vous pouvez l'activer.

Activez, désactivez ou modifiez une règle de trafic dans le profil application QoS

Vous ne pouvez pas ajouter ou supprimer une stratégie de trafic (c'est-à-dire une règle de trafic) du profil application QoS, mais vous pouvez modifier chaque règle de trafic pour l'adapter à votre situation réseau spécifique. Vous pouvez également activer ou désactiver des règles de trafic individuelles.

ATTENTION: Outre l'activation ou la désactivation des règles de trafic dans le profil application QoS, nous vous recommandons de modifier les paramètres des règles de trafic uniquement si vous en comprenez parfaitement les conséquences. Une configuration incorrecte peut entraîner des problèmes de connectivité pour tous les périphériques connectés ou tentant de se connecter à AP.

Pour activer, désactiver ou modifier une règle de trafic individuelle dans le profil application QoS :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.

   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> priorité du trafic**.

   La page s'ajuste.
6. Cliquez sur l'onglet **> application QoS**.

Le tableau des règles de circulation s'affiche. Par défaut, toutes les règles de trafic sont désactivées.

7. Si le profil application QoS est désactivé, cochez la case **application QoS**.
8. Cochez la case d'une règle de trafic, puis cliquez sur l'icône **en forme de crayon**.

   La fenêtre contextuelle Ajouter/modifier une règle s'affiche.
9. Réglez les paramètres suivants en fonction de vos besoins :
   a. Etat : Sélectionnez un bouton radio :
      - Activer. Après avoir cliqué sur le bouton appliquer, la règle prend effet si le profil application QoS est activé.
      - Désactiver : Vous pouvez modifier la règle, mais une fois que vous avez cliqué sur le bouton appliquer, la règle prise ne prend pas effet, même si le profil application QoS est activé. Par défaut, une règle est désactivée.

   b. Dans la section source, dans le champ **Port**, saisissez un numéro de port source auquel la règle de trafic doit s'appliquer.

      Le numéro de port doit être compris entre 1 et 65535.

   c. Dans la section destination, dans le champ **Port**, saisissez un numéro de port de destination auquel la règle de trafic doit s'appliquer.

      Le numéro de port doit être compris entre 1 et 65535.

   d. Cliquez sur le bouton **Apply** (Appliquer).

      La page application QoS s'affiche à nouveau.

Activez ou désactivez le profil application QoS

Par défaut, le profil application QoS est désactivé, de même que toutes les règles individuelles du profil application QoS. Une règle peut devenir active uniquement après avoir activé le profil application QoS et la règle (voir Activer, désactiver ou modifier une règle de trafic dans le profil application QoS à la page 178).

Pour activer ou désactiver application QoS :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.

   La page Traffic Policies s'affiche.

5. Cliquez sur l'onglet **> priorité du trafic**.

   La page s'ajuste.

6. Cliquez sur l'onglet **> application QoS**.

   La page application QoS s'affiche.

   REMARQUE: Pour activer application QoS, activez d'abord au moins une règle.

7. Cochez ou décochez la case **application QoS** :

   - cochée. Application QoS est activé.
   - **Case décochée**: Application QoS est désactivé.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Modifiez la priorité d'une règle de trafic dans le profil application QoS

Vous pouvez modifier la priorité d'une règle de trafic dans le profil application QoS.

Pour modifier la priorité d'une règle de trafic individuelle dans le profil application QoS :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.

   La page Traffic Policies s'affiche.

5. Cliquez sur l'onglet **> priorité du trafic**.

   La page s'ajuste.

6. Cliquez sur l'onglet **> application QoS**.

   Le tableau des règles de circulation s'affiche.

7. Si le profil application QoS est désactivé, cochez la case **Activer application QoS**.

8. Pointez sur l'icône **à six points** à gauche de la règle de trafic dont vous souhaitez modifier la priorité, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérer le profil de règle globale

Le profil règle globale est un profil personnalisable à l'échelle du système qui vous permet d'ajouter jusqu'à 50 règles application QoS personnalisées. Vous pouvez ajouter, modifier ou supprimer une règle dans le profil règle globale.

REMARQUE: Les règles du profil application QoS ont priorité sur les règles du profil règle globale.

Ajouter, modifier ou supprimer une règle du profil règle globale

Vous pouvez ajouter, modifier ou supprimer une règle du profil règle globale. Le profil règle globale peut prendre en charge jusqu'à 50 règles.

ATTENTION: Nous vous recommandons d'ajouter des règles uniquement si vous en comprenez parfaitement les conséquences. Une configuration incorrecte peut entraîner des problèmes de connectivité pour tous les périphériques connectés ou tentant de se connecter à AP.

Pour ajouter une règle globale au profil règle globale :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> priorité du trafic**.

   La page s'ajuste.
6. Cliquez sur l'onglet **> règle globale**.
   Le tableau des règles de circulation s'affiche. Si vous n'avez pas encore ajouté de règles, la table est vide.
7. Effectuez l'une des opérations suivantes :

   - Si vous souhaitez créer une règle, cliquez sur l'icône **plus**.
   - Si vous souhaitez modifier une règle, cochez la case correspondante, puis cliquez sur l'icône **en forme de crayon**.

La fenêtre contextuelle Ajouter/modifier une règle s'affiche.

8. Réglez les paramètres suivants en fonction de vos besoins :
   - Nom de la règle Vous pouvez modifier le nom de réseau par défaut. Ce qui suit s'applique au nom :
     - doit être un nom alphanumérique unique
     - peut contenir jusqu'à 32 caractères
     - ne peut inclure que les caractères spéciaux ', '-' et '_'
     - Doit commencer et se terminer par un caractère alphanumérique.
   - Etat : Sélectionnez un bouton radio :
     - Activer. Après avoir cliqué sur le bouton appliquer, la règle prend effet si le profil règle globale est activé. Il s'agit de l'option par défaut.
     - Désactiver : Vous pouvez modifier la règle, mais après avoir cliqué sur le bouton appliquer, la règle prise ne prend pas effet, même si le profil règle globale est activé.
   - Priorité du trafic Sélectionnez l'une des options suivantes dans le menu Vitesse :
     - Réseau Ce paramètre a la priorité la plus élevée.
     - **Voice**
     - **Vidéo**
     - **Arrière-plan**
     - **Meilleur effort**: Ce paramètre a la priorité la plus basse.
   - **Protocol** (Protocole). Dans le menu Protocole, sélectionnez le protocole.
     - **Tout**: La règle de circulation s'applique à tout trafic. Il s'agit de l'option par défaut.
     - **TCP**. La règle de trafic s'applique uniquement au trafic TCP (transmission Control Protocol).
     - **UDP**. La règle de trafic s'applique uniquement au trafic UDP (User Datagram Protocol).
     - **ICMP**: La règle de trafic s'applique uniquement au trafic ICMP (Internet Control message Protocol).
     - IGMP La règle de trafic s'applique uniquement au trafic ICMP (Internet Group Management Protocol).
   - **Source**. Pour définir la source du trafic auquel la règle de trafic doit s'appliquer, procédez comme suit :

a. Dans le menu **type**, sélectionnez l'une des options suivantes :

- **Tout**: Il s'agit de l'option par défaut. Ceci s'applique à toutes les adresses.
- **IP Address** (Adresse IP). La règle de trafic s'applique uniquement à l'adresse IP source que vous spécifiez dans le champ **adresse IP**.
- **Sous-réseau IP** : La règle de trafic s'applique uniquement au sous-réseau IP source que vous spécifiez dans les champs **adresse réseau** et **masque réseau**.

  La longueur du masque réseau doit être comprise entre 8 et 32 chiffres.

b. Dans le champ **Port**, saisissez un numéro de port source auquel la règle de trafic doit s'appliquer.

   Le numéro de port doit être compris entre 1 et 65535.

Le numéro de priorité s'ajuste.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

10. **Facultatif :** Pour supprimer une règle, cochez la case correspondante, puis cliquez sur l'icône **Supprimer**.

Activer ou désactiver le profil règle globale

Par défaut, le profil règle globale est désactivé. Une règle ne peut devenir active qu'après avoir activé le profil règle globale et la règle (voir Activer, désactiver ou modifier une règle de trafic dans le profil règle globale à la page 183).

Pour activer ou désactiver le profil règle globale :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

Vous gérez le AP via :

- **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

  REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.
   La page Traffic Policies s'affiche.
5. Cliquez sur l'onglet **> priorité du trafic**.

   La page s'ajuste.
6. Cliquez sur l'onglet **> règle globale**.

   La page règle globale s'affiche.

   REMARQUE: Pour activer le profil règle globale, activez d'abord au moins une règle.
7. Cochez ou décochez la case **règle globale** :
   - cochée. Le profil règle globale est activé.
   - **Case décochée**: Le profil règle globale est désactivé.
8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Modifiez la priorité d'une règle de trafic dans le profil règle globale

Vous pouvez modifier la priorité d'une règle de trafic dans le profil règle globale.

Pour modifier la priorité d'une règle de trafic individuelle dans le profil règle globale :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > stratégies de trafic**.

   La page Traffic Policies s'affiche.

5. Cliquez sur l'onglet **> priorité du trafic**.

   La page s'ajuste.

6. Cliquez sur l'onglet **> règle globale**.

   Le tableau des règles de circulation s'affiche.

7. Si le profil règle globale est désactivé, cochez la case **Activer la règle globale**.

8. Pointez sur l'icône **à six points** à gauche de la règle de trafic dont vous souhaitez modifier la priorité, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérez les listes de contrôle d'accès MAC basées sur SSID et les stratégies de trafic pour les réseaux WiFi

Outre les listes de contrôle d'accès MAC globales et les stratégies de trafic qui s'appliquent au trafic vers et depuis le LAN câblé (voir Gérez les listes de contrôle d'accès MAC globales et les stratégies de trafic à la page 152), le système AP prend en charge les listes de contrôle d'accès MAC et les stratégies de trafic basées sur le SSID qui vous permettent de contrôler quels clients WiFi peuvent se connecter à un réseau WiFi et quels trafics WiFi peuvent entrer et sortir d'un réseau WiFi :

- **Listes de contrôle d'accès MAC pour les clients WiFi** : Autoriser ou refuser aux clients WiFi de se connecter à un réseau WiFi en fonction de leur adresse MAC.

  Pour plus d'informations, consultez la section Gérer les listes de contrôle d'accès MAC pour les clients WiFi à la page 190.

- **Listes de contrôle d'accès MAC pour le trafic broadcast et multicast** : Autoriser le trafic de diffusion et de multidiffusion entrant uniquement à partir de périphériques spécifiques sur un réseau WiFi.

Pour plus d'informations, consultez la section Listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi à la page 198.

- Groupe de filtres de trafic MAC/IP Ajoutez des règles de trafic personnalisées à un groupe et appliquez le groupe à un réseau WiFi. Ces règles de trafic peuvent autoriser ou refuser le trafic en fonction de la couche réseau (adresses MAC ou IP) et d'un protocole sélectionné, et peuvent affecter le trafic WiFi entrant ou sortant, ou le trafic WiFi dans les deux sens.

  Pour plus d'informations, consultez la section Gérer les groupes de filtres de trafic MAC/IP pour les réseaux WiFi à la page 205.

  REMARQUE: Les règles de trafic globales du filtre de bruit sans fil (voir Gérer le filtre antibruit sans fil à la page 159) et, si activé, du filtre de trafic global (voir Gérer le filtre de trafic global à la page 167) ont une priorité plus élevée que les règles de trafic des groupes de filtre de trafic MAC/IP pour les réseaux WiFi.

Gérer les listes de contrôle d'accès MAC pour les clients WiFi

Le AP prend en charge huit listes de contrôle d'accès locales (ACL) qui vous permettent de contrôler quels clients WiFi sont autorisés à accéder et quels clients WiFi se voient refuser l'accès. Ces listes de contrôle d'accès sont basées sur des adresses MAC, et chaque liste de contrôle d'accès MAC locale peut contenir un nombre total de 512 adresses MAC.

Si vous configurez une liste de contrôle d'accès avec une stratégie autorisant l'accès et que vous appliquez cette liste de contrôle d'accès à un réseau WiFi (c'est-à-dire à un SSID), la liste de contrôle d'accès fonctionne comme suit :

- Un périphérique WiFi pour lequel vous placez l'adresse MAC dans la liste de contrôle d'accès est autorisé à accéder au réseau WiFi.
- Tous les autres appareils WiFi se voient refuser l'accès au réseau WiFi.

Si vous configurez une liste de contrôle d'accès avec une stratégie qui refuse l'accès et que vous appliquez cette liste de contrôle d'accès à un réseau WiFi (c'est-à-dire à un SSID), la liste de contrôle d'accès fonctionne comme suit :

- Un périphérique WiFi pour lequel vous placez l'adresse MAC dans la liste de contrôle d'accès se voit refuser l'accès au réseau WiFi.
- Tous les autres appareils WiFi sont autorisés à accéder au réseau WiFi.

Une liste de contrôle d'accès ne prend effet qu'une fois que vous l'avez appliquée à un réseau WiFi. Pour plus d'informations sur l'application d'une liste de contrôle d'accès pour les clients WiFi à un réseau WiFi, reportez-vous à la section Sélectionnez une liste

de contrôle d'accès MAC pour les clients WiFi dans un réseau WiFi à la page 321. Vous pouvez appliquer une ACL MAC pour les clients WiFi à plusieurs réseaux WiFi.

Les sections suivantes décrivent comment gérer les listes de contrôle d'accès MAC pour les clients WiFi :

- Configurez manuellement une ACL MAC pour les clients WiFi
- Importez une ACL MAC existante pour les clients WiFi

Configurez manuellement une ACL MAC pour les clients WiFi

Vous pouvez composer jusqu'à huit listes de contrôle d'accès (ACL) basées chacune sur un maximum de 512 adresses MAC. Le système AP inclut des listes de contrôle d'accès MAC avec les noms de groupe et paramètres par défaut suivants, que vous pouvez modifier :

- Administration Si cette option est activée, elle autorise l'accès aux stations approuvées par défaut.
- Invités : Si cette option est activée, elle autorise l'accès aux stations approuvées par défaut.
- **Invité 1**: Si cette option est activée, l'accès aux stations non fiables est refusé par défaut.
- Personnalisation Si cette option est activée, l'accès aux stations non fiables est refusé par défaut.
- **Personnalisé 1**: Si cette option est activée, elle autorise l'accès aux stations approuvées par défaut.
- **Personnalisé 2**: Si cette option est activée, elle autorise l'accès aux stations approuvées par défaut.
- **Personnalisé 3**: Si cette option est activée, elle autorise l'accès aux stations approuvées par défaut.
- **Personnalisé 4**: Si cette option est activée, elle autorise l'accès aux stations approuvées par défaut.

Par défaut, ces ACL MAC sont désactivées et n'incluent aucune station. Vous pouvez ajouter manuellement des périphériques, importer des périphériques (voir Importez une ACL MAC existante pour les clients WiFi à la page 194) ou effectuer les deux.

Vous pouvez utiliser une liste de contrôle d'accès MAC pour contrôler quels périphériques WiFi (stations) peuvent accéder à un réseau WiFi. Vous pouvez appliquer une ACL MAC à plusieurs réseaux WiFi.

Pour configurer manuellement une ACL MAC pour les clients WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > clients sans fil** .

   La page affiche toutes les ACL MAC.
5. Cliquez sur le nom de groupe de la liste de contrôle d'accès MAC que vous souhaitez configurer.

   La page MAC ACL s'affiche, affichant les paramètres de la MAC ACL sélectionnée.

   Les périphériques du tableau stations disponibles sont automatiquement détectés par le AP et sont communs à toutes les listes de contrôle d'accès MAC, ce qui vous

permet d'ajouter un périphérique à plusieurs listes de contrôle d'accès MAC. Une station voisine s'affiche comme voisine et une station connectée s'affiche comme connectée.

6. Pour modifier le nom du périphérique, entrez un nouveau nom dans le champ **Nom du périphérique**.

   Les noms de groupe par défaut pour les huit ACL MAC sont Management, Guest, Guest 1, Custom, Custom 1, Custom 2, Custom 3 et Custom 4.

   La longueur maximale des noms de rapports est de 32 caractères. Vous ne pouvez pas utiliser de caractères spéciaux à l'exception d'un tiret (-), d'un trait de soulignement (_) et d'un espace ( ). Le nom du groupe doit commencer et se terminer par des caractères alphanumériques.

7. Sélectionnez le bouton radio ACL Policy **Allow** ou **Deny**.

   Si vous sélectionnez le bouton radio **autoriser**, un périphérique WiFi pour lequel vous placez l'adresse MAC dans la liste de contrôle d'accès est autorisé à accéder au réseau WiFi, mais tous les autres périphériques WiFi se voient refuser l'accès au réseau WiFi.

   Si vous sélectionnez le bouton radio **refuser**, un périphérique WiFi pour lequel vous placez l'adresse MAC dans la liste de contrôle d'accès se voit refuser l'accès au réseau WiFi, mais tous les autres périphériques WiFi sont autorisés à accéder au réseau WiFi.

8. Composez la liste de contrôle d'accès de la manière suivante :

   - Pour une ACL pour laquelle vous avez sélectionné le bouton radio **autoriser** dans Étape 7, procédez comme suit :
     - Pour ajouter manuellement un périphérique au tableau stations de confiance, entrez l'adresse MAC au format 00-00-00-00-00-00 dans le champ situé sous le tableau stations de confiance, puis cliquez sur le bouton **Ajouter**.

       Le périphérique est ajouté au tableau stations de confiance.
     - Pour déplacer un périphérique du tableau stations disponibles vers le tableau stations approuvées, cochez la case correspondant au périphérique et cliquez sur le bouton **<< déplacer**.

       Vous pouvez effectuer une recherche dans le tableau stations disponibles. Vous pouvez également filtrer les périphériques dans le tableau stations disponibles en cliquant sur l'icône **de filtre**.
     - Pour supprimer un périphérique de la table stations de confiance, cochez la case correspondante et cliquez sur le bouton **Supprimer**.

       Vous pouvez effectuer une recherche dans le tableau stations de confiance.

Lorsque vous supprimez un périphérique du tableau stations approuvées, une fois que le système AP détecte à nouveau le périphérique, il est à nouveau placé dans le tableau stations disponibles.

- Pour une ACL pour laquelle vous avez sélectionné le bouton radio **refuser** dans Étape 7, procédez comme suit :
  - Pour ajouter manuellement un périphérique au tableau stations non fiables, entrez l'adresse MAC au format 00-00-00-00-00-00 dans le champ situé sous le tableau stations non fiables, puis cliquez sur le bouton **Ajouter**.

    Le périphérique est ajouté au tableau stations non fiables.
  - Pour déplacer un périphérique du tableau stations disponibles vers le tableau stations non approuvées, cochez la case correspondant au périphérique et cliquez sur le bouton **<< déplacer**.

    Vous pouvez effectuer une recherche dans le tableau stations disponibles. Vous pouvez également filtrer les périphériques dans le tableau stations disponibles en cliquant sur l'icône **de filtre**.
  - Pour supprimer un périphérique de la table stations non approuvées, cochez la case correspondante et cliquez sur le bouton **Supprimer**.

    Vous pouvez effectuer une recherche dans le tableau stations non fiables.

    Lorsque vous supprimez un périphérique du tableau stations non approuvées, une fois que le système AP détecte à nouveau le périphérique, il est à nouveau placé dans le tableau stations disponibles.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

   Pour plus d'informations sur l'application d'une liste de contrôle d'accès à un réseau WiFi, reportez-vous à la section Sélectionnez une liste de contrôle d'accès MAC pour les clients WiFi dans un réseau WiFi à la page 321.

   Les périphériques WiFi du tableau stations approuvées peuvent accéder au réseau WiFi auquel vous appliquez la liste de contrôle d'accès. Les périphériques WiFi du tableau stations non fiables ne peuvent pas accéder au réseau WiFi auquel vous appliquez la liste de contrôle d'accès.

Importez une ACL MAC existante pour les clients WiFi

Vous pouvez importer une liste de contrôle d'accès (ACL) existante basée sur un maximum de 512 adresses MAC. Vous pouvez importer la liste dans n'importe quelle liste de contrôle d'accès MAC, mais les adresses MAC de la liste ne sont disponibles que pour la liste de contrôle d'accès MAC dans laquelle vous importez la liste. Autrement

dit, si vous voulez utiliser la même liste dans une autre ACL MAC, vous devez également importer la liste dans cette ACL MAC.

Le fichier contenant les adresses MAC doit être au format suivant :

- Les entrées du fichier doivent être des adresses MAC au format hexadécimal, chaque octet étant séparé par un tiret, par exemple 00-11-22-33-44-55.
- Vous devez séparer les entrées par une virgule ou placer les entrées sur des lignes distinctes.
- Le fichier doit être au format texte (c'est-à-dire avec une extension `.txt` ou).

Vous pouvez utiliser une liste de contrôle d'accès MAC pour contrôler les périphériques WiFi qui peuvent accéder à un réseau WiFi. Vous pouvez appliquer une ACL MAC à plusieurs réseaux WiFi.

Pour importer une ACL MAC existante pour les clients WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > clients sans fil** .

   La page affiche toutes les ACL MAC.

5. Cliquez sur le nom de groupe de la liste de contrôle d'accès MAC que vous souhaitez configurer.

   La page MAC ACL s'affiche, affichant les paramètres de la MAC ACL sélectionnée.

   Les périphériques du tableau stations disponibles sont automatiquement détectés par le AP et sont communs à toutes les listes de contrôle d'accès MAC, ce qui vous permet d'ajouter un périphérique à plusieurs listes de contrôle d'accès MAC. Une station voisine s'affiche comme voisine et une station connectée s'affiche comme connectée.

6. Pour modifier le nom du périphérique, entrez un nouveau nom dans le champ **Nom du périphérique**.

   Les noms de groupe par défaut pour les huit ACL MAC sont Management, Guest, Guest 1, Custom, Custom 1, Custom 2, Custom 3 et Custom 4.

   Un nom de groupe peut contenir jusqu'à 32 caractères. Vous ne pouvez pas utiliser de caractères spéciaux à l'exception d'un tiret (-), d'un trait de soulignement (_) et d'un espace ( ).

7. Sélectionnez le bouton radio ACL Policy **Allow** ou **Deny**.

   Si vous sélectionnez le bouton radio **autoriser**, un périphérique WiFi pour lequel vous importez l'adresse MAC dans la liste de contrôle d'accès est autorisé à accéder au réseau WiFi, mais tous les autres périphériques WiFi se voient refuser l'accès au réseau WiFi.

   Si vous sélectionnez le bouton radio **refuser**, un périphérique WiFi pour lequel vous importez l'adresse MAC dans la liste de contrôle d'accès se voit refuser l'accès au réseau WiFi, mais tous les autres périphériques WiFi sont autorisés à accéder au réseau WiFi.

8. Pour télécharger un exemple d'ACL MAC au format requis pour l'importation, cliquez sur le lien **Télécharger un exemple**.

9. Importez et composez l'ACL de la manière suivante :

   - Pour une ACL pour laquelle vous avez sélectionné le bouton radio **autoriser** dans Étape 7, procédez comme suit :

a. Remplacez ou fusionnez les adresses MAC de la liste d'importation avec les adresses MAC du tableau stations approuvées (si elles figurent déjà dans le tableau) en sélectionnant l'un des boutons radio suivants :
   - Remplacer Les adresses MAC du tableau stations approuvées sont remplacées par celles de la liste d'importation.
   - **Fusionner**: Les adresses MAC du tableau stations approuvées sont fusionnées avec celles de la liste d'importation.

b. Cliquez sur le bouton **Parcourir** et naviguez jusqu'au fichier d'importation et sélectionnez-le.

   Les adresses MAC de la liste d'importation sont placées dans le tableau stations approuvées.

c. Pour supprimer une adresse MAC du tableau stations approuvées, sélectionnez l'adresse MAC et cliquez sur le bouton **Supprimer**.

   Vous pouvez effectuer une recherche dans le tableau stations de confiance.

   Lorsque vous supprimez un périphérique du tableau stations approuvées, une fois que le système AP détecte à nouveau le périphérique, il est à nouveau placé dans le tableau stations disponibles.

- Pour une ACL pour laquelle vous avez sélectionné le bouton radio **refuser** dans Étape 7, procédez comme suit :

  a. Remplacez ou fusionnez les adresses MAC de la liste d'importation avec les adresses MAC du tableau stations non fiables (si elles figurent déjà dans le tableau) en sélectionnant l'un des boutons radio suivants :
     - Remplacer Les adresses MAC de la table stations non fiables sont remplacées par celles de la liste d'importation.
     - **Fusionner**: Les adresses MAC de la table stations non fiables sont fusionnées avec celles de la liste d'importation.

  b. Cliquez sur le bouton **Parcourir** et naviguez jusqu'au fichier d'importation et sélectionnez-le.

     Les adresses MAC de la liste d'importation sont placées dans la table stations non fiables.

  c. Pour supprimer une adresse MAC du tableau stations non fiables, sélectionnez l'adresse MAC et cliquez sur le bouton **Supprimer**.

     Vous pouvez effectuer une recherche dans le tableau stations non fiables.

Lorsque vous supprimez un périphérique du tableau stations non approuvées, une fois que le système AP détecte à nouveau le périphérique, il est à nouveau placé dans le tableau stations disponibles.

10. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés. Pour plus d'informations sur l'ajout manuel d'adresses MAC à celles du tableau stations approuvées ou stations non approuvées, reportez-vous à la section Configurez manuellement une ACL MAC pour les clients WiFi à la page 191.

    Pour plus d'informations sur l'application d'une liste de contrôle d'accès à un réseau WiFi, reportez-vous à la section Sélectionnez une liste de contrôle d'accès MAC pour les clients WiFi dans un réseau WiFi à la page 321.

    Les périphériques WiFi du tableau stations approuvées peuvent accéder au réseau WiFi auquel vous appliquez la liste de contrôle d'accès. Les périphériques WiFi du tableau stations non fiables ne peuvent pas accéder au réseau WiFi auquel vous appliquez la liste de contrôle d'accès.

Listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi

Le AP prend en charge huit listes de contrôle d'accès locales (ACL) qui vous permettent de contrôler les clients WiFi autorisés à envoyer du trafic de diffusion et de multidiffusion vers un réseau WiFi (c'est-à-dire vers un SSID). Ces listes de contrôle d’accès sont basées sur des adresses MAC et chaque liste de contrôle d’accès MAC locale peut contenir un nombre total de 256 adresses MAC.
La liste de contrôle d'accès fonctionne comme suit :

- Un périphérique WiFi pour lequel vous placez l'adresse MAC dans la liste de contrôle d'accès est autorisé à envoyer du trafic de diffusion et de multidiffusion au réseau WiFi.

  Le trafic de diffusion et de multidiffusion est autorisé dans le même SSID sur lequel le client WiFi envoie le trafic, quelle que soit la radio sur laquelle le SSID est diffusé. Si un autre SSID utilise le même VLAN, les clients de l'autre SSID peuvent également recevoir le trafic de diffusion ou de multidiffusion.

  Par exemple :

  - Le SSID du « lobby principal » utilise VLAN 1 et diffuse sur la radio 2,4 GHz et la radio 5 GHz.
  - L'adresse MAC du client 1 se trouve sur la liste de contrôle d'accès MAC et le client 1 envoie le trafic de multidiffusion sur la radio 5 GHz du SSID du « lobby principal ».
  - Le SSID « Auditorium » est également configuré sur le même VLAN 1 et diffuse sur la radio 2,4 GHz.
  - Le SSID « Service comptabilité » est configuré sur VLAN 2 et diffuse sur la radio 2,4 GHz et la radio 5 GHz.

  Dans ce cas, le trafic multicast du client 1 peut atteindre tous les clients connectés au SSID du « lobby principal » ainsi que tous les clients connectés au SSID de « l'auditorium », mais il ne peut pas atteindre les clients connectés au SSID du « département comptable ».
- Le trafic de diffusion et de multidiffusion provenant de tous les autres appareils WiFi est rejeté par le réseau WiFi.

Une liste de contrôle d'accès ne prend effet qu'une fois que vous l'avez appliquée à un réseau WiFi. Pour plus d'informations sur l'application d'une liste de contrôle d'accès pour le trafic de diffusion et de multidiffusion à un réseau WiFi, reportez-vous à la section Sélectionnez une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi dans un réseau WiFi à la page 328. Vous pouvez appliquer une liste de contrôle d'accès pour le trafic de diffusion et de multidiffusion à plusieurs réseaux WiFi.

Les sections suivantes décrivent comment gérer les listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir de clients WiFi :

- Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi
- Importez une liste de contrôle d'accès MAC existante pour le trafic de diffusion et de multidiffusion à partir de clients WiFi

Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi

Vous pouvez composer jusqu'à huit listes de contrôle d'accès (ACL) pour le trafic de diffusion et de multidiffusion des clients WiFi. Chaque ACL est basée sur un maximum de 256 adresses MAC. Le système AP inclut des listes de contrôle d'accès MAC avec les noms de groupe par défaut Group 1 à Group 8. Vous pouvez modifier ces noms.

Par défaut, ces ACL MAC sont désactivées et n'incluent aucune station. Vous pouvez ajouter manuellement des périphériques, importer des périphériques (voir Importez

une liste de contrôle d'accès MAC existante pour le trafic de diffusion et de multidiffusion à partir de clients WiFi à la page 202) ou effectuer les deux.

Vous pouvez utiliser une liste de contrôle d'accès MAC pour contrôler quels clients WiFi (stations) sont autorisés à envoyer du trafic de diffusion et de multidiffusion vers un réseau WiFi (c'est-à-dire vers un SSID). Vous pouvez appliquer une ACL MAC à plusieurs réseaux WiFi.

Pour configurer manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir de clients WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > autoriser le trafic de diffusion/multidiffusion** .

La page autoriser le trafic de diffusion/multidiffusion s'affiche.

5. Cliquez sur le nom de groupe de la liste de contrôle d'accès MAC que vous souhaitez configurer.

   La page s'ajuste.

   Les périphériques du tableau stations connectées sont automatiquement détectés par le AP et sont communs à toutes les listes de contrôle d'accès MAC, ce qui vous permet d'ajouter un périphérique à plusieurs listes de contrôle d'accès MAC. Une station voisine s'affiche comme voisine et une station connectée s'affiche comme connectée.

6. Pour modifier le nom du périphérique, entrez un nouveau nom dans le champ **Nom du périphérique**.

   Les noms de groupe par défaut pour les huit listes de contrôle d'accès MAC sont Groupe 1, Groupe 2, Groupe 3, Groupe 4, Groupe 5, Groupe 6, Groupe 7 et Groupe 8.

   Un nom de groupe peut contenir jusqu'à 32 caractères. Vous ne pouvez pas utiliser de caractères spéciaux à l'exception d'un tiret (-), d'un trait de soulignement (_) et d'un espace ( ). Un nom de groupe doit commencer et se terminer par des caractères alphanumériques.

7. Composez la liste de contrôle d'accès de la manière suivante :

   - Pour ajouter manuellement un périphérique au tableau stations autorisées, entrez l'adresse MAC au format 00-00-00-00-00-00 dans le champ situé sous le tableau stations autorisées, puis cliquez sur le bouton **Ajouter**.

     Le périphérique est ajouté au tableau stations autorisées.

   - Pour déplacer un périphérique du tableau stations connectées au tableau stations autorisées, cochez la case correspondant au périphérique et cliquez sur le bouton **<< déplacer**.

     Vous pouvez effectuer une recherche dans le tableau stations connectées.

   - Pour supprimer un périphérique du tableau stations autorisées, cochez la case correspondante et cliquez sur le bouton **Supprimer**.

     Vous pouvez effectuer une recherche dans le tableau stations autorisées.

     Lorsque vous supprimez un périphérique du tableau stations autorisées, une fois que le système AP détecte à nouveau le périphérique, il est à nouveau placé dans le tableau stations connectées.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Pour plus d'informations sur l'application d'une liste de contrôle d'accès pour le trafic de diffusion et de multidiffusion des clients WiFi vers un réseau WiFi, reportez-vous à la section Sélectionnez une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi dans un réseau WiFi à la page 328.

Les périphériques WiFi du tableau stations autorisées sont autorisés à envoyer du trafic de diffusion et de multidiffusion vers un réseau WiFi auquel vous appliquez la liste de contrôle d'accès.

Importez une liste de contrôle d'accès MAC existante pour le trafic de diffusion et de multidiffusion à partir de clients WiFi

Vous pouvez importer une liste de contrôle d'accès (ACL) existante basée sur un maximum de 256 adresses MAC. Vous pouvez importer la liste dans n'importe quelle liste de contrôle d'accès MAC, mais les adresses MAC de la liste ne sont disponibles que pour la liste de contrôle d'accès MAC dans laquelle vous importez la liste. Autrement dit, si vous voulez utiliser la même liste dans une autre ACL MAC, vous devez également importer la liste dans cette ACL MAC.

Le fichier contenant les adresses MAC doit être au format suivant :

- Les entrées du fichier doivent être des adresses MAC au format hexadécimal, chaque octet étant séparé par un tiret, par exemple 00-11-22-33-44-55.
- Vous devez séparer les entrées par une virgule ou placer les entrées sur des lignes distinctes.
- Le fichier doit être au format texte (c'est-à-dire avec une extension `.txt` ou).

Vous pouvez utiliser une liste de contrôle d'accès MAC pour contrôler quels clients WiFi (stations) sont autorisés à envoyer du trafic de diffusion et de multidiffusion vers un réseau WiFi (c'est-à-dire vers un SSID). Vous pouvez appliquer une ACL MAC à plusieurs réseaux WiFi.

Pour importer une liste de contrôle d'accès MAC existante pour le trafic de diffusion et de multidiffusion à partir de clients WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > autoriser le trafic de diffusion/multidiffusion** .

   La page autoriser le trafic de diffusion/multidiffusion s'affiche.

5. Cliquez sur le nom de groupe de la liste de contrôle d'accès MAC que vous souhaitez configurer.

   La page s'ajuste.

   Les périphériques du tableau stations connectées sont automatiquement détectés par le AP et sont communs à toutes les listes de contrôle d'accès MAC, ce qui vous permet d'ajouter un périphérique à plusieurs listes de contrôle d'accès MAC. Une station voisine s'affiche comme voisine et une station connectée s'affiche comme connectée.

6. Pour modifier le nom du périphérique, entrez un nouveau nom dans le champ **Nom du périphérique**.

   Les noms de groupe par défaut pour les huit listes de contrôle d'accès MAC sont Groupe 1, Groupe 2, Groupe 3, Groupe 4, Groupe 5, Groupe 6, Groupe 7 et Groupe 8.

Un nom de groupe peut contenir jusqu'à 32 caractères. Vous ne pouvez pas utiliser de caractères spéciaux à l'exception d'un tiret (-), d'un trait de soulignement (_) et d'un espace ( ).

7. Pour télécharger un exemple d'ACL MAC au format requis pour l'importation, cliquez sur le lien **Télécharger un exemple**.
8. Importez et composez l'ACL de la manière suivante :
   a. Remplacez ou fusionnez les adresses MAC de la liste d'importation avec les adresses MAC du tableau stations autorisées (si elles figurent déjà dans le tableau) en sélectionnant l'un des boutons radio suivants :
      - Remplacer Les adresses MAC de la table stations autorisées sont remplacées par celles de la liste d'importation.
      - **Fusionner**: Les adresses MAC de la table stations autorisées sont fusionnées avec celles de la liste d'importation.

   b. Cliquez sur le bouton **Parcourir** et naviguez jusqu'au fichier d'importation et sélectionnez-le.

      Les adresses MAC de la liste d'importation sont placées dans le tableau stations autorisées.

   c. Pour supprimer une adresse MAC du tableau stations autorisées, sélectionnez l'adresse MAC et cliquez sur le bouton **Supprimer**.

      Vous pouvez effectuer une recherche dans le tableau stations autorisées.

      Lorsque vous supprimez un périphérique du tableau stations autorisées, une fois que le système AP détecte à nouveau le périphérique, il est à nouveau placé dans le tableau stations connectées.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

   Pour plus d'informations sur l'ajout manuel d'adresses MAC à celles du tableau stations autorisées, reportez-vous à la section Configurez manuellement une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi à la page 199.

   Pour plus d'informations sur l'application d'une liste de contrôle d'accès pour le trafic de diffusion et de multidiffusion des clients WiFi vers un réseau WiFi, reportez-vous à la section Sélectionnez une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi dans un réseau WiFi à la page 328.

   Les périphériques WiFi du tableau stations autorisées sont autorisés à envoyer du trafic de diffusion et de multidiffusion vers un réseau WiFi auquel vous appliquez la liste de contrôle d'accès.

Gérer les groupes de filtres de trafic MAC/IP pour les réseaux WiFi

Un groupe de filtres de trafic MAC/IP est un ensemble de règles de trafic IP et MAC personnalisées que vous pouvez appliquer au trafic entrant et sortant dans un réseau WiFi (SSID). Chaque règle peut autoriser ou refuser un type de trafic spécifique.

Le AP fournit huit groupes de filtres de trafic MAC/IP. Vous pouvez ajouter jusqu'à 16 règles de trafic à chaque groupe. Vous pouvez appliquer un seul groupe à plusieurs SSID.

REMARQUE: Les règles de trafic globales du filtre de bruit sans fil (voir Gérer le filtre antibruit sans fil à la page 159) et, si activé, du filtre de trafic global (voir Gérer le filtre de trafic global à la page 167) ont une priorité plus élevée que les règles de trafic des groupes de filtre de trafic MAC/IP pour les réseaux WiFi.

REMARQUE: Si vous appliquez un groupe de filtre de trafic MAC/IP à un réseau WiFi, le débit peut être affecté et peut être inférieur à la normale.

Les sections suivantes décrivent comment gérer les groupes de filtres de trafic MAC/IP :

- Activer ou désactiver un groupe de filtres de trafic MAC/IP
- Ajoutez une règle de trafic à un groupe de filtres de trafic MAC/IP
- Modifier une règle de trafic dans un groupe de filtres de trafic MAC/IP
- Modifiez la priorité d'une règle de trafic dans un groupe de filtres de trafic MAC/IP
- Supprimez une règle de trafic d'un groupe de filtres de trafic MAC/IP

Activer ou désactiver un groupe de filtres de trafic MAC/IP

Par défaut, un groupe filtre de trafic MAC/IP ne contient aucune stratégie de trafic (c'est-à-dire, des règles de trafic). Vous pouvez ajouter une règle (voir Ajoutez une règle de trafic à un groupe de filtres de trafic MAC/IP à la page 207), modifier une règle existante et supprimer une règle dont vous n'avez plus besoin.

La désactivation d'un groupe ne supprime pas les règles de trafic que vous avez ajoutées au groupe.

Pour activer ou désactiver un groupe de filtres de trafic MAC/IP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > filtres de trafic MAC/IP** .

   La page filtres de trafic MAC/IP s'affiche.

5. Cliquez sur le groupe que vous souhaitez activer ou désactiver.

   La page s'ajuste.

6. Cochez ou décochez la case **Activer le groupe**.

   - cochée. Le groupe est activé.
   - **Case décochée**: Le groupe est désactivé.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Ajoutez une règle de trafic à un groupe de filtres de trafic MAC/IP

Vous pouvez ajouter une ou plusieurs stratégies de trafic (c'est-à-dire des règles de trafic) à un groupe de filtres de trafic MAC/IP. La priorité des règles de trafic est attribuée dans l'ordre dans lequel vous ajoutez les règles. Autrement dit, la première règle que vous ajoutez se voit attribuer la première priorité (la plus élevée), la deuxième règle se voit attribuer la deuxième priorité, et ainsi de suite. Toutefois, vous pouvez modifier la priorité.

ATTENTION: Nous vous recommandons d'ajouter des règles de circulation uniquement si vous en comprenez parfaitement les conséquences. Une configuration incorrecte peut entraîner des problèmes de connectivité pour tous les périphériques connectés ou tentant de se connecter au réseau WiFi auquel vous appliquez le groupe filtre de trafic MAC/IP.

Pour ajouter une règle de trafic à un groupe de filtres de trafic MAC/IP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > filtres de trafic MAC/IP** .

   La page filtres de trafic MAC/IP s'affiche.

5. Cliquez sur le groupe auquel vous souhaitez ajouter une règle de trafic, puis cochez la case **Activer le groupe**.

6. Cliquez sur l'icône **plus**.

   La fenêtre contextuelle Ajouter/modifier une règle s'affiche.

7. Réglez les paramètres suivants en fonction de vos besoins :
   - Nom de la règle Vous pouvez modifier le nom de réseau par défaut. Ce qui suit s'applique au nom :
     - doit être un nom alphanumérique unique
     - peut contenir jusqu'à 32 caractères
     - ne peut inclure que les caractères spéciaux ', '-' et '_'
     - Doit commencer et se terminer par un caractère alphanumérique.
   - Etat : Sélectionnez un bouton radio :
     - Activer. Après avoir cliqué sur le bouton appliquer, la règle prend effet si le filtre de trafic MAC/IP est activé.
     - Désactiver : Vous pouvez modifier la règle, mais après avoir cliqué sur le bouton appliquer, la règle prise ne prend pas effet, même si le filtre de trafic MAC/IP est activé. Par défaut, une règle est désactivée.
   - Action : Sélectionnez un bouton radio :

- **Autoriser**. Le trafic qui correspond à la règle est autorisé à passer par le réseau WiFi.
- Refuser Le trafic correspondant à la règle est abandonné.

- Direction Sélectionnez un bouton radio :
  - po. La règle de trafic s'applique uniquement au trafic entrant à partir d'un réseau WiFi.
  - **Sortie**: Les règles de trafic s'appliquent uniquement au trafic sortant vers un réseau WiFi.
  - **Les deux**: La règle de trafic s'applique à la fois au trafic entrant à partir d'un réseau WiFi et au trafic sortant à destination d'un réseau WiFi.
- **Couche réseau** : Sélectionnez un bouton radio :
  - MAC : La règle de trafic filtre les paquets au niveau MAC.
  - IP : La règle de trafic filtre les paquets au niveau IP.
- **Protocol** (Protocole). Dans le menu Protocole, sélectionnez le protocole.
  - **Tout**: La règle de circulation s'applique à tout trafic.
  - ARP La règle de trafic s'applique uniquement au trafic ARP (Address Resolution Protocol).
  - **TCP**. La règle de trafic s'applique uniquement au trafic TCP (transmission Control Protocol).
  - **UDP**. La règle de trafic s'applique uniquement au trafic UDP (User Datagram Protocol).
  - **ICMP**: La règle de trafic s'applique uniquement au trafic ICMP (Internet Control message Protocol).
  - IGMP La règle de trafic s'applique uniquement au trafic ICMP (Internet Group Management Protocol).
- **Source**. Pour définir la source du trafic auquel la règle de trafic doit s'appliquer, procédez comme suit :
  a. Dans le menu **type**, sélectionnez le type d'adresse MAC ou IP source, en fonction de la couche réseau (MAC ou IP) sélectionnée :
     - **Tout**: La règle de trafic est appliquée à toute adresse MAC ou IP source.
     - **Adresse MAC** (niveau MAC uniquement) : La règle de trafic s'applique uniquement à l'adresse MAC source que vous spécifiez dans le champ **adresse MAC**.

- **Adresse IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement à l'adresse IP source que vous spécifiez dans le champ **adresse IP**.
- **Sous-réseau IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement au sous-réseau IP source que vous spécifiez dans les champs **adresse réseau** et **masque réseau**.

  La longueur du masque réseau doit être comprise entre 8 et 32 chiffres.

b. Dans le champ **Port**, saisissez un numéro de port source auquel la règle de trafic doit s'appliquer.

   Le numéro de port doit être compris entre 1 et 65535.

- Destination Pour définir la destination du trafic auquel la règle de trafic doit s'appliquer, procédez comme suit :

  a. Dans le menu **type**, sélectionnez le type d'adresse MAC ou IP de destination, en fonction de la couche réseau (MAC ou IP) sélectionnée :

  - **Tout**: La règle de trafic est appliquée à toute adresse MAC ou IP de destination.
  - **Adresse MAC** (niveau MAC uniquement) : La règle de trafic s'applique uniquement à l'adresse MAC de destination que vous spécifiez dans le champ **adresse MAC**.
  - **Adresse IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement à l'adresse IP de destination que vous spécifiez dans le champ **adresse IP**.
  - **Sous-réseau IP** (niveau IP uniquement) : La règle de trafic s'applique uniquement au sous-réseau IP de destination que vous spécifiez dans les champs **adresse réseau** et **masque réseau**.

    La longueur du masque réseau doit être comprise entre 8 et 32 chiffres.

  b. Dans le champ **Port**, saisissez un numéro de port de destination auquel la règle de trafic doit s'appliquer.

     Le numéro de port doit être compris entre 1 et 65535.

8. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK**.

   La page filtres de trafic MAC/IP s'affiche à nouveau.

9. Pour modifier la priorité de la règle de trafic, pointez sur l'icône **à six points** à gauche de la règle de trafic, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.

   Le numéro de priorité s'ajuste.

10. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

Modifier une règle de trafic dans un groupe de filtres de trafic MAC/IP

Vous pouvez modifier une règle de trafic existante dans un groupe filtre de trafic MAC/IP.

Pour modifier une règle de trafic existante dans un groupe de filtres de trafic MAC/IP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > filtres de trafic MAC/IP** .

   La page filtres de trafic MAC/IP s'affiche.

5. Cliquez sur le groupe dans lequel vous souhaitez modifier une règle de trafic.

   Le tableau indique les règles de trafic que vous avez ajoutées au groupe.

6. Si le groupe est désactivé, cochez la case **Activer le groupe**.

7. Cochez la case de la règle de trafic, puis cliquez sur l'icône **en forme de crayon**.

   La fenêtre contextuelle Ajouter/modifier une règle de trafic s'affiche.

8. Modifiez les paramètres en fonction de vos besoins.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Ajoutez une règle de trafic à un groupe de filtres de trafic MAC/IP à la page 207.

9. Dans la fenêtre qui s'ouvre, cliquez sur le bouton **OK**.

   La page filtres de trafic MAC/IP s'affiche à nouveau.

10. Pour modifier la priorité de la règle de trafic, pointez sur l'icône **à six points** à gauche de la règle de trafic, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.

    Le numéro de priorité s'ajuste.

11. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

Modifiez la priorité d'une règle de trafic dans un groupe de filtres de trafic MAC/IP

Vous pouvez modifier la priorité d'une règle de trafic dans un groupe filtre de trafic MAC/IP.

Pour modifier la priorité d'une règle de trafic dans un groupe de filtres de trafic MAC/IP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > filtres de trafic MAC/IP** .

La page filtres de trafic MAC/IP s'affiche.

5. Cliquez sur le groupe dans lequel vous souhaitez modifier la priorité d'une règle de trafic.

   Le tableau des règles de circulation s'affiche.

6. Si le groupe est désactivé, cochez la case **Activer le groupe**.
7. Pointez sur l'icône **à six points** à gauche de la règle de trafic dont vous souhaitez modifier la priorité, cliquez et maintenez le bouton enfoncé, puis déplacez la règle de trafic vers le haut ou vers le bas dans le tableau.

   Le numéro de priorité s'ajuste.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Supprimez une règle de trafic d'un groupe de filtres de trafic MAC/IP

Vous pouvez supprimer une règle de trafic dont vous n'avez plus besoin.

Pour supprimer une règle de trafic d'un groupe de filtres de trafic MAC/IP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > listes de contrôle d'accès > filtres de trafic MAC/IP** .

   La page filtres de trafic MAC/IP s'affiche.
5. Cliquez sur le groupe dont vous souhaitez supprimer une règle de trafic.

   Le tableau des règles de circulation s'affiche.
6. Si le groupe est désactivé, cochez la case **Activer le groupe**.
7. Cochez la case de la règle de trafic, puis cliquez sur l'icône de **la corbeille**.

   La règle de trafic est supprimée.
8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer la sécurité L2

La sécurité L2 peut empêcher les attaques via l'empilement VLAN en bloquant les paquets marqués VLAN sur l'interface WiFi. Si vous activez la sécurité L2, le système AP autorise uniquement certains types de trafic client, tels que le trafic ARP, IPv4 et IPv6, sur n'importe quel réseau WiFi. La sécurité L2 est désactivée par défaut.

Pour activer la sécurité L2 :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > sécurité > sécurité L2** .

   La page sécurité L2 s'affiche.
5. Sélectionnez la case d'option **Oui**.

   Par défaut, le bouton radio non est sélectionné et la sécurité L2 est désactivée.
6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérer la protection contre les dénis de service

Une attaque par déni de service (dos) est une tentative de rendre un ordinateur ou une ressource réseau inaccessible aux utilisateurs prévus. La protection DOS surveille et filtre le trafic entrant pour prévenir les attaques par inondation qui pourraient submerger les ressources système. Par défaut, la protection dos est désactivée. Lorsque vous activez la prévention dos, vous pouvez configurer les options de filtrage des attaques par inondation suivantes :

- **Filtrage des attaques ICMP-Flood** : Activez ce paramètre pour vous protéger contre les attaques ICMP Flood (ping floods).
- **Filtrage des attaques TCP-SYN-Flood** : Activez ce paramètre pour vous protéger contre les attaques TCP SYN flood qui peuvent épuiser les ressources de connexion.
- **Filtrage des attaques UDP-Flood** : Activez ce paramètre pour limiter les attaques UDP Flood qui peuvent consommer de la bande passante.

Pour gérer les paramètres de prévention dos et configurer les options de filtrage des attaques par inondation :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sécurité > prévention dos** .

   La page prévention dos s'affiche.
5. Sélectionnez un bouton radio prévention dos :
   - Activer. La prévention DOS est activée.
   - Désactiver : La prévention DOS est désactivée. Il s'agit de l'option par défaut.
6. Sélectionnez un bouton radio prévention dos ICMP-Flood Attack Filtering :
   - Activer. Le filtrage des attaques ICMP-flood est activé.
   - Désactiver : Le filtrage des attaques ICMP-flood est désactivé. Il s'agit de l'option par défaut.

   Si vous activez cette option, dans le champ de droite, définissez le seuil de paquet d'attaque ICMP-flood entre 5 et 7200 pour supprimer le trafic excédentaire dépassant cette limite.
7. Sélectionnez un bouton radio prévention dos TCP-SYN-Flood Attack Filtering :
   - Activer. Le filtrage des attaques TCP-SYN-flood est activé.
   - Désactiver : Le filtrage des attaques TCP-SYN-flood est désactivé. Il s'agit de l'option par défaut.

   Si vous activez cette option, dans le champ de droite, définissez le seuil de paquet d'attaque TCP-SYN-flood entre 5 et 7200 pour supprimer le trafic excédentaire dépassant cette limite.
8. Sélectionnez un bouton radio filtrage des attaques UDP-Flood de prévention dos :

- Activer. Le filtrage des attaques UDP-Flood est activé.
- Désactiver : Le filtrage des attaques UDP-Flood est désactivé. Il s'agit de l'option par défaut.

Si vous activez cette option, dans le champ de droite, définissez le seuil de paquet d'attaque UDP-flood entre 5 et 7200 pour supprimer le trafic excédentaire dépassant cette limite.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

9

Gérer le réseau local et les paramètres IP

Ce chapitre décrit comment gérer le réseau local (LAN) et les paramètres IP du AP.

Ce chapitre comprend les sections suivantes :

- Désactivez le client DHCP et définissez une adresse IP fixe
- Activez le client DHCP
- Définissez le VLAN de gestion et de VLAN 802.1Q
- Définissez un nom de domaine existant
- Activer ou désactiver le protocole Spanning Tree
- Activer ou désactiver la fonction de vérification de l'intégrité du réseau
- Activer ou désactiver igmp snooping
- Activer ou désactiver le chemin de données assisté par matériel
- Activer ou désactiver Ethernet LLDP
- Activer ou désactiver UPnP
- Gérer la passerelle DNS multicast

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Désactivez le client DHCP et définissez une adresse IP fixe

Par défaut, le client DHCP du APest activé et le AP reçoit une adresse IP d'un serveur DHCP (ou d'un routeur fonctionnant comme un serveur DHCP) de votre réseau. Si votre réseau n'inclut pas de serveur DHCP ou si vous préférez spécifier une adresse IP fixe (statique), désactivez le client DHCP du AP.

Pour désactiver le client DHCP et définir une adresse IP fixe :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > IP > LAN**.

   La page Paramètres IPv4 s'affiche. Les champs sont masqués car le client DHCP est activé.

5. Sélectionnez le bouton radio **désactiver**.

   Les champs ne sont pas masqués.

6. Spécifiez les paramètres comme décrit dans le tableau suivant.

Paramètre	Description
Adresse IP	Adresse IP dans la plage utilisée par votre réseau local. Par défaut, l'adresse IP du routeur est 192.168.0.100.
Masque de sous-réseau	Le masque de sous-réseau doit être compatible avec votre réseau local. Par défaut, le masque réseau est 255.255.255.0.
Passerelle	Adresse IP de la passerelle sur votre réseau local.
DNS primaire	Adresse IP du serveur DNS (Domain Name System) principal sur votre réseau local.
DNS secondaire	Adresse IP du serveur DNS secondaire sur votre réseau local ou laissez ce champ vide.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Le AP redémarre avec les nouveaux paramètres IP.

Activez le client DHCP

Par défaut, le client DHCP du APest activé et le AP reçoit une adresse IP d'un serveur DHCP (ou d'un routeur fonctionnant comme un serveur DHCP) de votre réseau.

Si vous avez désactivé le client DHCP, vous pouvez le réactiver.

Pour activer le client DHCP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > IP > LAN**.

   La page Paramètres IPv4 s'affiche.

5. Sélectionnez le bouton radio Activer.

   Les champs sont masqués.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Le AP redémarre avec les nouveaux paramètres IP. Il peut s'écouler un certain temps avant que le AP reçoive son paramètre d'adresse IP du serveur DHCP.

Définissez le VLAN de gestion et de VLAN 802.1Q

Le protocole VLAN 802.1Q sur le système APsépare logiquement le trafic sur le même réseau physique (câblé). Ce protocole peut fonctionner avec des VLAN balisés et non balisés, comme suit :

- **Untagged VLAN** : APEnvoie des trames non marquées à partir de son interface Ethernet. Les trames non balisées entrantes sont attribuées au VLAN non balisé. Par défaut, le VLAN non balisé est VLAN 1. Par défaut, le AP fonctionne avec un VLAN non balisé.
- **Tagged VLAN** : Le AP identifie toutes les trames qu'il envoie depuis son interface Ethernet. Seules les trames entrantes étiquetées avec des ID VLAN connus sont acceptées.

Le VLAN de gestion permet de gérer le trafic tel que le trafic Telnet, SNMP, HTTP et HTTPS envoyé vers et depuis le AP. Les trames qui appartiennent au VLAN de gestion et qui sont envoyées sur la jonction ne reçoivent pas d'en-tête 802.1Q. Si un port est membre d'un seul VLAN, son trafic peut être déétiqueté.

Un VLAN de gestion autre que le VLAN 1 par défaut et les fonctionnalités suivantes s'excluent mutuellement :

- Passerelle mDNS (voir Gérer la passerelle DNS multicast à la page 235)
- Mode NAT (voir Définissez le mode NAT ou Bridge pour l'adressage et le trafic à la page 315)

Pour définir le VLAN de gestion et de VLAN 802.1Q :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

- **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

  REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > IP > LAN**.

   La page Paramètres IPv4 s'affiche.

5. Pour modifier le VLAN 802.1Q, décochez ou cochez la case **VLAN non balisé** :

   - **Untagged VLAN** : Par défaut, la case **VLAN non balisé** est cochée. APEnvoie des trames non marquées à partir de son interface Ethernet. Les trames non balisées entrantes sont attribuées au VLAN non balisé. Par défaut, le VLAN non balisé est VLAN 1, mais vous pouvez entrer un autre ID VLAN dans le champ si cet ID VLAN est pris en charge sur votre réseau.
   - **Tagged VLAN** : Désélectionnez la case **Untagged VLAN** (VLAN non étiqueté) uniquement si les concentrateurs et commutateurs de votre réseau prennent en charge la norme VLAN (802.1q). Le AP identifie toutes les trames qu'il envoie depuis son interface Ethernet. Seules les trames entrantes étiquetées avec des ID VLAN connus sont acceptées. De même, modifiez l'ID du VLAN non étiqueté uniquement si les concentrateurs et commutateurs de votre réseau local prennent en charge le protocole VLAN 802.1Q et si le nouvel ID VLAN est pris en charge sur votre réseau.

   Un ID VLAN doit être compris entre 1 et 4094.

6. Pour modifier l'ID VLAN du VLAN de gestion, entrez un autre ID VLAN dans le champ **VLAN de gestion**.

Par défaut, l'VLAN de gestion est VLAN 1. Si vous modifiez l'ID VLAN, assurez-vous que l'ID VLAN est pris en charge sur votre réseau.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Le AP redémarre avec les nouveaux paramètres VLAN.

Définissez un nom de domaine existant

Vous pouvez spécifier un nom de domaine complet (FQDN) existant pour le AP afin de pouvoir accéder au système AP à l'aide d'un nom de domaine au lieu d'une adresse IP.

Le nom de domaine complet doit être un nom de domaine enregistré auprès d'un fournisseur DNS (Domain Name System).
Voici les conditions requises pour le nom de domaine complet :

- La longueur maximale du nom de domaine complet est de 255 caractères, avec un maximum de 63 caractères par étiquette, séparés par un point (.) entre chaque étiquette.
- Les caractères alphanumériques sont autorisés (a–z et 1–9).
- Un espace n'est pas autorisé.
- Un point (.) et un tiret (-) sont autorisés mais le nom ne peut commencer par aucun des deux.
- Les chiffres et les caractères spéciaux ne sont pas autorisés dans le dernier libellé du nom de domaine complet.

Un exemple est *myap01-firstfloor-myorganization.com*.

Pour définir un nom de domaine complet existant :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > IP > LAN**.

   La page Paramètres IPv4 s'affiche.

5. Dans le champ **nom de domaine complet**, spécifiez le nom de domaine complet.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Le AP tente de résoudre le FDQN en une adresse IP.

Activer ou désactiver le protocole Spanning Tree

Pour les emplacements où plusieurs APsont actifs et où des chemins réseau redondants peuvent être présents, le protocole STP (Spanning Tree Protocol) peut empêcher les boucles réseau. Si votre emplacement peut inclure des chemins réseau redondants, nous vous recommandons d'activer le protocole STP.

Pour activer ou désactiver le protocole Spanning Tree :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > général**.

   La page General (Général) s'affiche.
5. Sélectionnez un bouton radio Spanning Tree Protocol :
   - Activer. STP est activé.
   - Désactiver : STP est désactivé. Il s'agit de l'option par défaut.
6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer ou désactiver la fonction de vérification de l'intégrité du réseau

La fonction de vérification de l'intégrité du réseau permet au AP de vérifier si la liaison en amont est active avant que le AP autorise les associations WiFi. Assurez-vous que la passerelle par défaut est correctement configurée. Par défaut, la fonction de vérification de l'intégrité du réseau est désactivée.

Pour activer ou désactiver la fonction de vérification de l'intégrité du réseau :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > général**.

   La page General (Général) s'affiche.
5. Sélectionnez un bouton radio vérification de l'intégrité du réseau :
   - Activer. La fonction de vérification de l'intégrité du réseau est activée.
   - Désactiver : La fonction de vérification de l'intégrité du réseau est désactivée. Il s'agit de l'option par défaut.
6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer ou désactiver igmp snooping

igmp snooping permet de transmettre des paquets de multidiffusion IP uniquement aux membres d'un groupe de multidiffusion correspondant. L'activation de igmp snooping empêche l'inondation du trafic de multidiffusion vers tous les ports d'un domaine de broadcast. Par défaut, igmp snooping est désactivé sur le AP.

Pour activer ou désactiver igmp snooping :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > général**.

   La page General (Général) s'affiche.
5. Sélectionnez un bouton radio igmp snooping :
   - Activer. igmp snooping est activé.
   - Désactiver : igmp snooping est désactivé. Il s'agit de l'option par défaut.
6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer ou désactiver le chemin de données assisté par matériel

Le chemin de données assisté par matériel, qui est activé par défaut, augmente le débit maximal sur le AP.

Nous vous recommandons de laisser le chemin de données assisté par matériel activé, sauf si vous devez activer le routage inter-VLAN ou prendre en charge les trames Jumbo dans le réseau. La désactivation du chemin de données assisté par matériel réduit le débit maximal, mais le débit reste suffisamment élevé pour un déploiement en entreprise.

Pour activer ou désactiver le chemin de données assisté par matériel :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > général**.

   La page General (Général) s'affiche.
5. Sélectionnez un bouton radio chemin de données assisté par matériel :
   - Activer. Le chemin de données assisté par matériel est activé. Il s'agit de l'option par défaut.
   - Désactiver : Le chemin de données assisté par matériel est désactivé.
6. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Activer ou désactiver Ethernet LLDP

Le protocole LLDP (Link Layer Discovery Protocol), tel que spécifié dans la norme IEEE 802.1AB, peut fournir des messages de couche de liaison aux périphériques réseau adjacents. Par exemple, LLDP permet aux périphériques réseau tels que les commutateurs et les périphériques de gestion de découvrir APdans un réseau.

LLDP peut également détecter si le AP est alimenté via PoE. Par défaut, LLDP est activé.

Pour activer ou désactiver LLDP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > Ethernet LLDP**.

   La page Ethernet LLDP s'affiche.

5. Sélectionnez un bouton radio :
   - Activer. LLDP est activé. Il s'agit de l'option par défaut.
   - Désactiver : LLDP est désactivé.

   ATTENTION: Si le AP est alimenté par un commutateur PoE et que vous désactivez le protocole LLDP, l'alimentation du AP peut être coupée après avoir cliqué sur le bouton **appliquer**. Dans ce cas, redémarrez AP.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer ou désactiver UPnP

Universal Plug and Play (UPnP) permet à d'autres périphériques d'un réseau prenant en charge UPnP de découvrir leAP. UPnP est activé par défaut.

Pour activer ou désactiver UPnP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > UPnP**.

   La page UPnP s'affiche.

5. Sélectionnez un bouton radio :
   - Activer. UPnP est activé. Il s'agit de l'option par défaut.
   - Désactiver : UPnP est désactivé.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérer la passerelle DNS multicast

Le AP peut fonctionner comme une passerelle DNS multicast (mDNS) pour permettre le partage de périphériques et de services sur différents VLAN et réseaux WiFi. MDNS fonctionne même si le routage inter-VLAN est désactivé sur le réseau auquel est connecté leAP.

Les périphériques partagés comprennent les imprimantes, les scanners, les périphériques de stockage et autres périphériques matériels. Les services comprennent de multiples services de téléphonie, de musique et de diffusion vidéo, des services de partage de fichiers et d'autres services et applications.

Par exemple, si un groupe de clients se trouve sur VLAN 20 et qu'une imprimante se trouve sur VLAN 1, une passerelle mDNS peut rendre l'imprimante détectable par les clients. Ou, si un participant à une réunion souhaite utiliser un téléphone connecté à un réseau WiFi sur VLAN 20 pour diffuser une présentation sur un appareil grand écran

connecté à un réseau WiFi sur VLAN 30, une autre stratégie de passerelle mDNS peut le rendre possible.

Un service peut s'exécuter sur un périphérique filaire ou WiFi, mais pour qu'un client WiFi puisse accéder au service, le client WiFi doit être connecté à un réseau WiFi sur un système sur APlequel la fonction de passerelle mDNS est activée.

Dans un réseau comportant plusieurs périphériques prenant en charge la fonctionnalité de passerelle mDNS, vous pouvez définir un périphérique, tel qu'un routeur, comme réflecteur mDNS, qui réannonce les périphériques et services partagés sur l'ensemble du réseau.

Une passerelle mDNS et les fonctionnalités suivantes s'excluent mutuellement :

- Sécurité WPA2 entreprise et sécurité WPA3 entreprise utilisant un VLAN dynamique (voir Configurez un réseau WiFi ouvert ou sécurisé à la page 73)
- Multi PSK (voir Configurez Multi PSK pour un réseau WiFi à la page 97)
- Management VLAN (voir Définissez le VLAN de gestion et de VLAN 802.1Q à la page 224)
- Mode NAT (voir Définissez le mode NAT ou Bridge pour l'adressage et le trafic à la page 315)
- Isolation du client (voir Activer ou désactiver l'isolation client pour un réseau WiFi à la page 317)

Activez la passerelle DNS de multidiffusion et ajoutez une stratégie

Après avoir activé la passerelle DNS multicast (mDNS) et ajouté une stratégie, APpeut détecter automatiquement les périphériques et les services qui peuvent être partagés. La stratégie forme un pont entre les deux VLAN suivants :

- **Service VLAN** : Le VLAN qui inclut des périphériques ou des services partagés en tant que membres. Par exemple, le type de périphérique partagé peut être *imprimante*, auquel cas le service VLAN est l'VLAN dont l'imprimante est membre.

  Ou, le type de service partagé peut être *Googlecast*, auquel cas le service VLAN est le VLAN dont le périphérique Googlecast est membre.
- **VLAN sur les réseaux WiFi autorisés** : Le VLAN qui inclut en tant que membres les périphériques WiFi qui doivent être en mesure d'utiliser les périphériques partagés ou le service sur le VLAN de service.

Vous pouvez ajouter jusqu'à huit stratégies. Une stratégie permet d'accéder à un périphérique ou service partagé. Un client WiFi peut accéder à un périphérique ou

service partagé si APune stratégie est configurée pour le périphérique de service partagé.

Pour activer la passerelle DNS multicast et ajouter une stratégie :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > passerelle mDNS** .

   La page Configuration de la passerelle mDNS s'affiche.
5. Sélectionnez le bouton radio **Activer** la passerelle mDNS.

   Par défaut, la passerelle mDNS est désactivée et le bouton radio désactiver est sélectionné.

6. Si votre réseau comprend plusieurs APs qui prennent en charge la fonctionnalité de passerelle mDNS et que celle-ci AP doit fonctionner comme réflecteur mDNS APdans votre réseau, sélectionnez le bouton radio **Oui**.

   Par défaut, le bouton radio Ethernet est sélectionné.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Une section contenant des informations sur la stratégie s'affiche.

8. Cliquez sur le bouton Ajouter une stratégie **+**.

   Une ligne est ajoutée au tableau avec les stratégies de passerelle mDNS. (Vous pouvez ajouter plusieurs lignes pour plusieurs stratégies.)

9. Définissez la stratégie de passerelle mDNS en spécifiant les éléments suivants :
   - Nom de la politique Nom permettant d'identifier la stratégie. Vous pouvez utiliser jusqu'à 32 caractères alphanumériques et spéciaux, à l'exception des guillemets doubles (« ») et des barres obliques inverses (\).
   - **Services partagés** : Dans le menu **services partagés**, sélectionnez le type de périphérique (par exemple, imprimante) ou de service (par exemple, Googlecast) à partager.
   - **Service VLAN** : Dans le champ **VLAN du service**, entrez l'ID VLAN qui inclut comme membres le type de périphérique ou de service partagé que vous sélectionnez dans le menu **services partagés**.

     L'ID VLAN peut être compris entre 1 et 4094.
   - **Service IP** : Entrez l'adresse IP du périphérique ou du service partagé que vous sélectionnez dans le menu **services partagés**.
   - **Réseau WiFi autorisé** : Dans le menu **réseau WiFi autorisé**, sélectionnez les réseaux WiFi et leurs VLAN associés, qui incluent en tant que membres les périphériques WiFi qui doivent être en mesure d'utiliser le type de périphérique partagé ou de service que vous sélectionnez dans le menu **services partagés**.

10. Pour ajouter une autre stratégie mDNS, cliquez sur le bouton Ajouter une stratégie **+** et répétez l'étape précédente.

11. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

Modifier ou supprimer une stratégie DNS de multidiffusion

Vous pouvez modifier ou supprimer une stratégie DNS multicast (mDNS).

Pour modifier ou supprimer une stratégie mDNS :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > passerelle mDNS** .

   La page Configuration de la passerelle mDNS s'affiche.
5. Pour modifier une stratégie :

a. Cliquez sur l'icône **crayon et bloc-notes** à droite de la stratégie.

b. Modifiez les paramètres.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Activez la passerelle DNS de multidiffusion et ajoutez une stratégie à la page 236.

c. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

6. Pour supprimer une stratégie :

   a. Cliquez sur l'icône de **la corbeille** à droite de la stratégie.

   b. Confirmez la suppression.

10

Gérer et entretenir le AP

Ce chapitre décrit comment gérer et maintenir le AP.

Ce chapitre comprend les sections suivantes :

- Changez le mode de gestion en Netgear insight ou navigateur Web
- Modifiez le pays ou la région d'exploitation
- Modifiez le mot de passe du compte utilisateur admin
- Modifiez le nom du système
- Spécifiez un serveur NTP personnalisé
- Définissez le fuseau horaire
- Gérer les paramètres syslog
- Gérer le micrologiciel du AP
- Gérer le fichier de configuration du AP
- Utilisez le bouton Réinitialiser pour redémarrer le AP
- Redémarrez APà partir de l'interface utilisateur du périphérique
- Programmez le redémarrage duAP
- Rétablissez les paramètres par défaut du routeur
- Activez SNMP et gérez les paramètres SNMP
- Gérer la LED
- Gérer le mode efficacité énergétique
- Configurez le mode de puissance d'entrée PoE

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Changez le mode de gestion en Netgear insight ou navigateur Web

Le AP peut fonctionner dans l'un des modes de gestion suivants :

- Netgear insight (Cloud/distant) Pour les abonnés Netgear insight Premium et Insight Pro, vous pouvez gérer APà distance via le portail cloud Insight ou à partir d'un appareil mobile sur lequel l'application Netgear insight est installée.

  Le mode Netgear insight est le paramètre par défaut. Dans ce mode, vous *pouvez* vous connecter à APvia l'interface utilisateur du terminal, mais seule une interface utilisateur de base et limitée est disponible. Pour plus d'informations sur le portail cloud Netgear insight et l'application Insight, rendez-vous sur le site netgear.com/business/services/insight/subscription et consultez la base de connaissances NETGEAR à l'adresse netgear.com/support/product/insight.aspx.

  ATTENTION: Lorsque vous passez du mode navigateur Web au mode Netgear insight, la configuration de APest réinitialisée (effacée) à l'exception de l'adresse IP, du AP nom et du mot de passe de l'interface utilisateur du périphérique. APRedémarre et diffuse le SSID Netgear xxxxxx, dans lequel xxxxxx représente les six derniers chiffres hexadécimaux de APl'adresse MAC du système. L'adresse MAC est indiquée sur l'étiquette du produit. La phrase de passe WiFi par défaut est **sharedsecret**.

- **Navigateur Web (local)**: Vous pouvez gérer APlocalement à partir d'un périphérique WiFi ou filaire via l'interface utilisateur du périphérique. Dans ce mode, APfonctionne comme un périphérique autonome et n'est pas connecté à la plate-forme de gestion basée sur le cloud Insight.

  REMARQUE: Si vous ajoutez d'abord APà un emplacement réseau Netgear insight et gérez APvia le portail cloud Insight ou l'application Insight, puis que vous passez en mode navigateur Web, vous devez continuer à utiliser le mot de passe réseau Insight pour accéder à l'interface utilisateur du terminal jusqu'à ce que vous modifiiez manuellement le mot de passe administrateur sur AP.

Pour passer du mode de gestion au mode Netgear insight ou au mode navigateur Web :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > basique > mode gestion** .

   La page mode de gestion s'affiche.

5. Sélectionnez l'une des cases d'option suivantes :
   - Netgear insight (Cloud/distant) Les AP fonctions en mode de gestion Netgear insight.
   - **Navigateur Web (local)**: Les AP fonctions en mode de gestion du navigateur Web.

ATTENTION: Lorsque vous passez du mode navigateur Web au mode Netgear insight, la configuration de APest réinitialisée (effacée) à l'exception de l'adresse IP, du AP nom et du mot de passe de l'interface utilisateur du périphérique. APRedémarre et diffuse le SSID Netgear xxxxxx, dans lequel xxxxxx représente les six derniers chiffres hexadécimaux de APl'adresse MAC du système. L'adresse MAC est indiquée sur l'étiquette du produit. La phrase de passe WiFi par défaut est **sharedsecret**.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. Le AP redémarre dans le nouveau mode de gestion.

Modifiez le pays ou la région d'exploitation

Vous pouvez modifier le pays ou la région dans lequel opère leAP. Notez ce qui suit :

- Dans certains pays, le PA est vendu avec un paramètre Pays/Région préconfiguré et vous ne pouvez pas le modifier.
- si votre pays ou région ne figure pas dans le menu, mettez à jour le micrologiciel du PA, puis revérifiez. Si votre pays ou votre région ne figure toujours pas dans la liste, contactez l'assistance NETGEAR.
- vérifiez que le pays est défini sur l'emplacement où l'appareil est installé. L'utilisation du routeur dans une région autre que celle indiquée ici peut être interdite par la loi. Vous êtes responsable de la conformité aux réglementations locales, régionales et nationales définies pour les canaux, les niveaux de puissance et les plages de fréquences.

Pour modifier le pays ou la région d'exploitation :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations,

consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Système > Base**.

   La page Général affiche les paramètres système de base.

5. Sélectionnez un pays ou une région dans le menu **pays / région**.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. Le AP redémarre avec les paramètres Wi-Fi et radio par défaut spécifiques au pays ou à la région sélectionné.

Modifiez le mot de passe du compte utilisateur admin

Ce mot de passe de compte d'utilisateur admin est le mot de passe que vous utilisez pour vous connecter à l'interface utilisateur du terminal de APavec le nom d'utilisateur admin. (Il ne s'agit pas de la phrase de passe que vous utilisez pour accéder au WiFi.)

Le mot de passe doit comporter entre 8 et 64 caractères et contenir au moins une lettre majuscule, une lettre minuscule et un chiffre.

Pour définir le mot de passe du nom d'utilisateur admin :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > comptes utilisateur**.
   La page qui s'affiche vous permet de modifier les comptes d'utilisateur.
5. En regard de admin, dans le champ **Password**, entrez le nouveau mot de passe.
6. Dans le champ **confirmer le mot de** passe, entrez le même nouveau mot de passe.

   REMARQUE: (Vous ne pouvez pas modifier le nom d’utilisateur.) Le nom doit rester admin.
7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. La prochaine fois que vous vous connecterez à AP, vous devrez utiliser le nouveau mot de passe. Si vous oubliez le nouveau mot de passe, vous devez rétablir les paramètres par défaut duAP. Cela restaure le mot de passe par défaut.

Modifiez le nom du système

Le nom du système (également appelé APnom, ou nom du point d'accès) est un nom NetBIOS unique pour le AP. Le nom du système par défaut se trouve sur l'APétiquette. Par défaut, le nom du système est Netgear xxxxxx, dans lequel xxxxxx représente les six derniers chiffres hexadécimaux de APl'adresse MAC du système.

Pour modifier le nom du système :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Système > Base**.

   La page Général affiche les paramètres système de base.

5. Entrez un nouveau nom dans le champ Nom (SSID).

   Respectez les consignes suivantes :

   - Le nom doit contenir des caractères alphanumériques, peut contenir des tirets et ne peut pas dépasser 64 caractères.
   - Le nom ne peut pas commencer ou se terminer par un tiret.
   - Le nom doit contenir au moins un caractère alphabétique.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Spécifiez un serveur NTP personnalisé

Par défaut, le système AP reçoit son heure d'un serveur NTP (Network Time Protocol) NETGEAR par défaut, mais vous pouvez également spécifier un serveur NTP personnalisé.

Pour spécifier un serveur NTP personnalisé :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **Gestion > Configuration > Système > Base**.

   La page heure s'affiche.

   Par défaut, le bouton radio Activer est sélectionné et APfonctionne comme un client NTP qui reçoit son heure d'un serveur NTP NETGEAR par défaut.
5. Cochez la case **utiliser un serveur NTP personnalisé**.
6. Effectuez l'une des actions suivantes :
   - Entrez le nom d'hôte du serveur NTP.

Par défaut, le bouton radio Ethernet est sélectionné.

- Sélectionnez le bouton radio **adresse IP** et entrez l'adresse IP du serveur NTP.

7. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Lorsque le AP se connecte via Internet au nouveau serveur NTP, la date et l'heure qui s'affichent sur la page sont ajustées en fonction de vos paramètres.

   Pour plus d'informations sur la définition du fuseau horaire, reportez-vous à la section Définissez le fuseau horaire à la page 250.

Définissez le fuseau horaire

Lorsque le AP synchronise son horloge avec un serveur NTP (Network Time Protocol), la page affiche la date et l'heure. Si la page n'affiche pas la date et l'heure correctes, vous devrez peut-être définir le fuseau horaire.

Pour définir le fuseau horaire :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Système > Base**.

   La page qui s'affiche vous permet de modifier les paramètres de l'heure.

5. Dans le menu **fuseau horaire**, sélectionnez le fuseau horaire de la zone dans laquelle fonctionne leAP.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés. Lorsque le AP se connecte via Internet à un serveur NTP, la date et l'heure qui s'affichent sur la page sont ajustées en fonction de vos paramètres.

   Pour plus d'informations sur les autres paramètres de l'heure, reportez-vous à la section Spécifiez un serveur NTP personnalisé à la page 248.

Gérer les paramètres syslog

Si un serveur syslog est présent sur votre réseau, vous pouvez configurer APpour qu'il envoie ses journaux système au serveur syslog.

Pour gérer les paramètres syslog et activer la fonction syslog :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > Syslog**.

   La page Syslog s'affiche.

5. Pour activer la fonction de serveur syslog, cochez la case **Activer syslog**.

6. Spécifiez l'adresse IP et le numéro de port du serveur syslog :

   - Adresse IP du serveur Syslog Entrez l'adresse IP du serveur syslog sur votre réseau.
   - Numéro de port Entrez le numéro de port auquel le syslog peut être atteint. Le numéro de port doit être compris entre 1 et 65535. Par défaut, le numéro de port est 514.

7. Vous pouvez configurer les niveaux de gravité du serveur syslog pour consigner les messages aux niveaux prévus. Cette fonctionnalité améliore la gestion des journaux en activant le filtrage en fonction de l'importance des données des journaux. Pour

configurer le niveau syslog, déplacez le curseur **niveau syslog** sur l'une des options suivantes :

- **Urgence**
- **Erreur**
- **Avertissement**
- **Informations**
- **Débogage**

REMARQUE: Si vous sélectionnez un niveau syslog, tous les niveaux syslog inférieurs à ce niveau sont également inclus. Par exemple, si vous sélectionnez avertissement, les messages Info et Debug log sont également inclus.

8. Pour consigner les informations collectées auprès des périphériques qui recherchent activement des connexions réseau sur le serveur syslog configuré, cochez la case **Log Probing clients**.

   Le message de journal utilise le format suivant :

   ```
   Probe request-Client:<aa:bb:cc:dd:ee:ff>, SSID: <Name>, BSSID:
   <aa:bb:cc:dd:ff:ee>, RSSI: <-xx dbM>, Radio: <x>, Channel: <y>
   ```

   Les champs d'un message de journal signifient ce qui suit :

   - Demande de sonde-client : adresse MAC
   - SSID : Nom
   - BSSID adresse MAC
   - RSSI : Valeur négative en dBm
   - Radio Valeur en GHz
   - Canal : Valeur en GHz

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérer le micrologiciel du AP

Le AP micrologiciel est stocké dans la mémoire flash.

Vous pouvez vérifier si un nouveau micrologiciel est disponible et mettre à jour le AP vers le nouveau micrologiciel. Vous pouvez également visiter le site Web d'assistance NETGEAR, télécharger manuellement le micrologiciel sur un ordinateur local et mettre

à jour le AP vers le nouveau micrologiciel. Si quelqu'un (généralement l'administrateur réseau) place un nouveau micrologiciel sur un serveur FTP sécurisé (SFTP) du réseau, vous pouvez charger le micrologiciel à partir du serveur et mettre à jour le micrologiciel du AP.

Selon la manière dont vous êtes connecté au AP, nous vous recommandons les méthodes de mise à jour du micrologiciel suivantes :

- Connexion WiFi Si vous êtes connecté via WiFi au AP, laissez APvérifier sur Internet si un nouveau micrologiciel est disponible. Consultez la section Laissez le AP rechercher un nouveau micrologiciel et mettez-le à jour à la page 254.

  Avec cette méthode, si un nouveau micrologiciel est disponible, il est téléchargé directement sur le AP.
- Connexions réseau local Si vous êtes connecté via le LAN au AP, mettez à jour manuellement le micrologiciel à partir d'un ordinateur ou d'un serveur SFTP. Consultez la section Téléchargez manuellement le micrologiciel et mettez à jour le AP à la page 256 ou Utilisez un serveur SFTP pour mettre à jour AP à la page 260.

  Avec ce mode, si un nouveau micrologiciel est disponible, vous devez soit le télécharger sur votre ordinateur, puis le télécharger sur le APAP, soit le télécharger à partir d'un serveur SFTP sur le .

Les sections suivantes décrivent les méthodes de gestion du micrologiciel :

- Laissez le AP rechercher un nouveau micrologiciel et mettez-le à jour
- Téléchargez manuellement le micrologiciel et mettez à jour le AP
- Revenez au micrologiciel de sauvegarde
- Utilisez un serveur SFTP pour mettre à jour AP

Laissez le AP rechercher un nouveau micrologiciel et mettez-le à jour

Pour que vous puissiez laisser le AP rechercher un nouveau micrologiciel, le AP doit être connecté à Internet.

Pour laisser le AP rechercher un nouveau micrologiciel et mettre à jour le AP:

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations,

consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l'appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s'affiche.

4. Cliquez sur le bouton **Check for Updates** (Rechercher des mises à jour).

   Le AP détecte le nouveau micrologiciel, le cas échéant, et affiche la dernière version disponible.

5. Pour lire les notes de version, le cas échéant, cliquez sur le lien **Notes de version**.

   Une page Web affiche les notes de version.

6. Pour télécharger et installer le nouveau micrologiciel, cliquez sur le bouton **mettre à niveau maintenant** et suivez les invites et les boîtes de dialogue.

   Le PA localise le firmware, le télécharge et démarre la mise à jour.

   Avertissement: pour éviter tout risque de corruption du micrologiciel (firmware), n'interrompez pas la mise à jour. Par exemple, ne fermez pas le navigateur, ne cliquez pas sur un lien et ne chargez pas de nouvelle page. N'éteignez pas le PA. Patientez jusqu'à ce que le APredémarre et que le voyant reste vert fixe ou bleu fixe.

La procédure de chargement du firmware prend plusieurs minutes. Une fois la mise à jour achevée, le AP redémarre.

7. Vérifiez que le AP exécute la nouvelle version du micrologiciel en vous reconnectant au AP.

   La version du micrologiciel s'affiche sur le tableau de bord.

8. Lisez les notes de mise à jour du nouveau micrologiciel pour déterminer si vous devez reconfigurer le AP après la mise à jour.

Téléchargez manuellement le micrologiciel et mettez à jour le AP

Le téléchargement du micrologiciel sur un ordinateur local et la mise à jour du AP sont deux tâches distinctes qui sont combinées dans la procédure suivante. Après avoir mis à jour le AP vers le nouveau micrologiciel, l'ancien micrologiciel est enregistré en tant que micrologiciel de sauvegarde afin que vous puissiez y revenir (voir Revenez au micrologiciel de sauvegarde à la page 258).

ATTENTION: Lorsque vous installez une version antérieure du micrologiciel (ou la version de sauvegarde du micrologiciel), c'est-à-dire que vous rétrogradez plutôt que de mettre à jour le micrologiciel, la configuration du AP est réinitialisée (effacée) à l'exception de l'adresse IP, AP du nom et du mot de passe de l'interface utilisateur du périphérique. APRedémarre et diffuse le SSID Netgear xxxxxx, dans lequel xxxxxx représente les six derniers chiffres hexadécimaux de APl'adresse MAC du système. L'adresse MAC est indiquée sur l'étiquette du produit. La phrase de passe WiFi par défaut est **sharedsecret**.

Pour télécharger manuellement le micrologiciel et mettre à jour AP:

1. Rendez-vous sur netgear.com/support/download/, recherchez la page d'assistance de votre produit et téléchargez le nouveau micrologiciel.
2. Lisez les notes de mise à jour du nouveau micrologiciel pour déterminer si vous devez reconfigurer APaprès la mise à niveau.
3. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
4. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

5. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

6. Sélectionnez **gestion > maintenance > mise à niveau > mise à niveau du micrologiciel** .

   La page mise à niveau du micrologiciel s'affiche.

7. Assurez-vous que **local** est sélectionné dans le menu **Options de mise à niveau**.

   Local est la sélection par défaut.

8. Localisez et sélectionnez le fichier du micrologiciel sur votre ordinateur en procédant comme suit :

   a. Cliquez sur le bouton **Browse** (Parcourir).

   b. Naviguez jusqu'au fichier du micrologiciel.

      Le nom du fichier se termine par `.tar` .

   c. Sélectionnez le fichier du micrologiciel.

9. Cliquez sur le bouton **mettre à niveau**.

Avertissement: pour éviter tout risque de corruption du micrologiciel (firmware), n'interrompez pas la mise à jour. Par exemple, ne fermez pas le navigateur, ne cliquez pas sur un lien et ne chargez pas de nouvelle page. N'éteignez pas le PA. Patientez jusqu'à ce que le APredémarre et que le voyant reste vert fixe ou bleu fixe.

La procédure de chargement du firmware prend plusieurs minutes. Une fois la mise à jour achevée, le AP redémarre.

10. Vérifiez que le AP exécute la nouvelle version du micrologiciel en vous reconnectant au AP.

    La version du micrologiciel s'affiche sur le tableau de bord.

Revenez au micrologiciel de sauvegarde

Après avoir mis à niveau le AP vers le nouveau micrologiciel, l'ancien micrologiciel est enregistré en tant que micrologiciel de sauvegarde afin que vous puissiez y revenir.

ATTENTION: Lorsque vous revenez au micrologiciel de sauvegarde et que la version du micrologiciel de sauvegarde est antérieure à la version du micrologiciel exécutée sur le AP, la configuration du AP est réinitialisée (effacée) à l'exception de l'adresse IP, du AP nom et du mot de passe de l'interface utilisateur du périphérique. APRedémarre et diffuse le SSID Netgear xxxxxx, dans lequel xxxxxx représente les six derniers chiffres hexadécimaux de APl'adresse MAC du système. L'adresse MAC est indiquée sur l'étiquette du produit. La phrase de passe WiFi par défaut est **sharedsecret**.

Pour revenir au micrologiciel de sauvegarde sur le AP:

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

- **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

  REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > maintenance > mise à niveau > mise à niveau du micrologiciel** .

   La page mise à niveau du micrologiciel s'affiche. La page affiche la version actuelle du micrologiciel et la version de sauvegarde du micrologiciel.

5. Cliquez sur le bouton **Boot Up Backup Firmware**.

   Une fenêtre d'avertissement s'affiche.

   ATTENTION: Lorsque vous revenez au micrologiciel de sauvegarde, la configuration du AP est réinitialisée (effacée), à l'exception de l'adresse IP, AP du nom et du mot de passe de l'interface utilisateur du périphérique. APRedémarre et diffuse le SSID Netgear xxxxxx, dans lequel xxxxxx représente les six derniers chiffres hexadécimaux de APl'adresse MAC du système. L'adresse MAC est indiquée sur l'étiquette du produit. La phrase de passe WiFi par défaut est **sharedsecret**.

6. Cliquez sur le bouton **permuter**.

   La fenêtre contextuelle se ferme, le processus de réversion du micrologiciel démarre et APredémarre.

Avertissement: Pour éviter tout risque de corruption du micrologiciel (firmware), n'interrompez pas la mise à jour. Par exemple, ne fermez pas le navigateur, ne cliquez pas sur un lien et ne chargez pas de nouvelle page. N'éteignez pas le PA. Patientez jusqu'à ce que le APredémarre et que le voyant reste vert fixe ou bleu fixe.

7. Vérifiez que le AP exécute la version de sauvegarde du micrologiciel en vous reconnectant au AP.

   La version du micrologiciel s'affiche sur le tableau de bord.

Utilisez un serveur SFTP pour mettre à jour AP

Si quelqu'un (généralement l'administrateur réseau) place un nouveau micrologiciel sur un serveur FTP sécurisé (SFTP) du réseau, vous pouvez charger le micrologiciel à partir du serveur SFTP et mettre à jour le micrologiciel du AP.

Pour mettre à jour le micrologiciel du AP à partir d'un serveur SFTP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > maintenance > mise à niveau > mise à niveau du micrologiciel** .

   La page mise à niveau du micrologiciel s'affiche.

5. Dans le menu **Options de mise à niveau** , sélectionnez **SFTP**.
6. Spécifiez les paramètres de serveur suivants :
   - **Fichier de micrologiciel** : Nom du APfichier de micrologiciel sur le serveur SFTP.
   - **Adresse IP du serveur SFTP** : Adresse IP du serveur SFTP sur votre réseau.
   - Nom d'utilisateur : Nom d'utilisateur requis pour accéder au serveur SFTP.
   - Nouveau mot de passe : Mot de passe requis pour accéder au serveur SFTP.
7. Cliquez sur le bouton **mettre à niveau**.

   Avertissement: pour éviter tout risque de corruption du micrologiciel (firmware), n'interrompez pas la mise à jour. Par exemple, ne fermez pas le navigateur, ne cliquez pas sur un lien et ne chargez pas de nouvelle page. N'éteignez pas le PA. Patientez jusqu'à ce que le APredémarre et que le voyant reste vert fixe ou bleu fixe.

   La procédure de chargement du firmware prend plusieurs minutes. Une fois la mise à jour achevée, le AP redémarre.
8. Vérifiez que le AP exécute la nouvelle version du micrologiciel en vous reconnectant au AP.

   La version du micrologiciel s'affiche sur le tableau de bord.

Gérer le fichier de configuration du AP

Les paramètres de configuration du routeur sont stockés dans le routeur dans un fichier de configuration. Vous pouvez sauvegarder (enregistrer) ce fichier sur votre ordinateur ou le restaurer.

Sauvegardez la configuration :

Vous pouvez enregistrer une copie des paramètres de configuration actuels. Si nécessaire, vous pouvez restaurer les paramètres de configuration ultérieurement.

REMARQUE: Le fichier de sauvegarde est sauvegardé dans un format binaire de sorte qu'il est protégé et ne peut pas être ouvert par une application normale.

Pour sauvegarder les paramètres de configuration du routeur :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > maintenance > mise à niveau > sauvegarde et restauration > Paramètres de sauvegarde** .

   La page Paramètres de sauvegarde s'affiche.

5. Cliquez sur le bouton **Backup** (Sauvegarder).

   Une fenêtre contextuelle s'affiche.

6. Entrez un mot de passe pour protéger le fichier de sauvegarde, puis cliquez sur le bouton **continuer**.

   Vous pouvez utiliser votre mot de passe existant (celui que vous utilisez pour vous connecter au AP) ou saisir un mot de passe unique.

   Le mot de passe doit comporter entre 8 et 64 caractères et contenir au moins une lettre majuscule, une lettre minuscule et un chiffre. Les caractères spéciaux suivants sont autorisés :

   ! @ # $ % ^ & * ( )

   REMARQUE: Nous vous recommandons d'enregistrer le mot de passe car vous devez le saisir à nouveau si vous restaurez la configuration à partir du fichier de sauvegarde.

7. Choisissez un emplacement pour stocker le fichier sur votre ordinateur.

   Le nom du fichier de sauvegarde peut être `WBE7XX-NETGEARYYYYYY-dd-mm-yy_hh-mm-ss-config.tar` ou `WBE7XX-WBE7XX-YYYYYY-dd-mm-yy_hh-mm-ss-config.tar` .

7XX représente le numéro de modèle, AAAA représente les six derniers chiffres hexadécimaux de APl'adresse MAC du (ou le nom du système), jj la date, mm le mois, aa l'année, hh l'heure (au format 24 heures), mm les minutes et ss les secondes.

Des exemples de nom de fichier de sauvegarde sont `WBE7XX-NETGEAR1A2B3C-02-18-24_16-44-12-config.tar` et `WBE7XX-WBE7XX-1A2B3C-02-18-24_16-44-12-config.tar` .

8. Suivez les instructions de votre navigateur pour enregistrer le fichier.

Restaurez la AP configuration

Si vous avez sauvegardé le fichier de configuration d'un routeur, vous pouvez restaurer la configuration à partir de ce fichier.

Pour restaurer les paramètres de configuration que vous avez sauvegardés :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > maintenance > mise à niveau > sauvegarde et restauration > restaurer les paramètres**.

   La page restaurer les paramètres s'affiche.

5. Cliquez sur le bouton **Parcourir** et naviguez jusqu'au fichier de configuration enregistré et sélectionnez-le.

   Le nom du fichier de sauvegarde peut être `WBE7XX-NETGEARYYYYYY-dd-mm-yy_hh-mm-ss-config.tar` ou `WBE7XX-WBE7XX-YYYYYY-dd-mm-yy_hh-mm-ss-config.tar` .

   7XX représente le numéro de modèle, AAAA représente les six derniers chiffres hexadécimaux de APl'adresse MAC du (ou le nom du système), jj la date, mm le mois, aa l'année, hh l'heure (au format 24 heures), mm les minutes et ss les secondes.

   Des exemples de nom de fichier de sauvegarde sont `WBE7XX-NETGEAR1A2B3C-02-18-24_16-44-12-config.tar` et `WBE7XX-WBE7XX-1A2B3C-02-18-24_16-44-12-config.tar` .

6. Cliquez sur le bouton **Restore** (Restaurer).

   Une fenêtre contextuelle s'affiche.

7. Entrez le mot de passe que vous avez spécifié lors de l'enregistrement du fichier de sauvegarde, puis cliquez sur le bouton **continuer**.

8. Cliquez sur le bouton **Restore** (Restaurer).

   La fenêtre contextuelle se ferme et la configuration est téléchargée sur le routeur. Une fois la restauration terminée, le routeur redémarre. Ce processus prend environ deux minutes.

   Avertissement: Pour éviter tout risque de corruption du micrologiciel (firmware), n'interrompez pas la mise à jour. Par exemple, ne fermez pas le navigateur, ne cliquez pas sur un lien et ne chargez pas de nouvelle page. N'éteignez pas le PA. Patientez jusqu'à ce que le APredémarre et que le voyant s'allume en vert ou en bleu.

Utilisez le bouton Réinitialiser pour redémarrer le AP

Vous pouvez utiliser le bouton **Réinitialiser** pour redémarrer le AP.

Pour redémarrer le AP à l'aide du bouton Réinitialiser :

1. Sur le panneau inférieur du AP, repérez le bouton de **réinitialisation** encastré.
2. À l'aide d'un trombone déplié, appuyez sur le bouton de **réinitialisation** et maintenez-le enfoncé pendant environ deux secondes jusqu'à ce que le voyant s'allume en orange fixe, puis relâchez immédiatement le bouton.

   ATTENTION: Si vous continuez à maintenir le bouton **Réinitialiser** enfoncé, il est possible que le APrétablisse ses paramètres par défaut. Relâchez le bouton dès que le voyant s'allume en orange fixe.

   Le AP redémarre, ce qui prend environ deux minutes.

   Avertissement: Pour éviter tout risque de corruption du micrologiciel (firmware), n'interrompez pas la mise à jour. N'éteignez pas le PA. Patientez jusqu'à ce que le APredémarre et que le voyant s'allume en vert ou en bleu.

Redémarrez APà partir de l'interface utilisateur du périphérique

Si vous ne pouvez pas accéder physiquement au AP pour le redémarrer (c'est-à-dire, déconnecter l'alimentation et la reconnecter), vous pouvez utiliser l'interface utilisateur du périphérique pour redémarrer le AP.

Pour redémarrer APà partir de l'interface utilisateur du périphérique :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations,

consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > maintenance > Réinitialiser > redémarrer AP**.

   La page redémarrer AP s'affiche.

5. Cliquez sur le bouton **redémarrer AP**.

   Une fenêtre d'avertissement s'affiche.

6. Cliquez sur **le** bouton redémarrer.

   La fenêtre contextuelle se ferme et APredémarre, ce qui prend environ une minute.

Programmez le redémarrage duAP

Vous pouvez programmer le redémarrage du système APà un moment plus pratique pour le réseau, par exemple, lorsque vous ne vous attendez pas à ce qu'aucun client WiFi (ou seulement quelques-uns) soit connecté au AP. Le planning que vous configurez est un planning récurrent.

Pour programmer le redémarrage du AP:

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > maintenance > Réinitialiser > redémarrer AP**.

   La page redémarrer AP s'affiche.
5. Cliquez sur le bouton **Activer redémarrage programmé** pour qu'il s'affiche en bleu.

   Les commandes de planification s'affichent.
6. Cochez la case correspondant au jour où vous souhaitez que le système APredémarre.

   Vous pouvez sélectionner plusieurs jours.

7. A l'aide des menus **Start Time**, spécifiez l'heure et les minutes auxquelles le système AP doit redémarrer.

   Spécifiez l'heure au format 24 heures.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Rétablissez les paramètres par défaut du routeur

Dans certaines circonstances (par exemple, si vous avez perdu la trace des modifications apportées aux paramètres du routeur ou si vous déplacez le routeur vers un autre réseau), vous pouvez effacer la configuration et restaurer les paramètres par défaut du routeur.

Si vous ne connaissez pas l'adresse IP actuelle du AP, essayez d'abord d'utiliser une application de scanner IP pour détecter l'adresse IP avant de réinitialiser APles paramètres par défaut du.

REMARQUE: Vous pouvez également utiliser l'application Netgear insight pour découvrir l'adresse IP attribuée au AP. Pour plus d'informations, consultez la section Connectez-vous via WiFi à l'aide de l'application Netgear insight à la page 34.

Pour rétablir les paramètres par défaut duAP, vous pouvez utiliser le bouton **Réinitialiser** du APou la fonction **Réinitialiser de** l'interface utilisateur du périphérique. Toutefois, si vous ne trouvez pas l'adresse IP ou si vous avez perdu le mot de passe pour accéder au AP, vous devez utiliser le bouton **Réinitialiser** .

Après avoir réinitialisé les paramètres par défaut du systèmeAP, le mot de passe du nom d'utilisateur administrateur est **password**, APle client DHCP du est activé, le SSID de configuration est affiché au format NETGEARxxxxxx-SETUP et le mot de passe par défaut pour l'accès WiFi est **sharedsecret**. Si le AP ne reçoit pas d'adresse IP d'un serveur DHCP, l'adresse IP LAN est définie sur 192.168.0,100.

Pour obtenir une liste complète des paramètres usine par défaut, reportez-vous à la section Paramètres par défaut à la page 382.

Utilisez le bouton DE RÉINITIALISATION pour réinitialiser le commutateur AP

Vous pouvez utiliser le bouton **DE RÉINITIALISATION** pour rétablir les paramètres par défaut du commutateur.

ATTENTION: Ce processus efface tous les paramètres que vous avez configurés dans le routeur.

Pour rétablir les paramètres par défaut du routeur :

1. Sur le panneau inférieur du AP, repérez le bouton de **réinitialisation** encastré.
2. À l'aide d'un trombone déplié, appuyez sur le bouton de **réinitialisation** et maintenez-le enfoncé jusqu'à ce que le voyant clignote en orange.

   REMARQUE: Si vous maintenez le bouton de **réinitialisation** enfoncé, le voyant s'allume d'abord en orange fixe, puis clignote en orange environ 5 secondes plus tard. Si vous relâchez le bouton alors que le voyant est orange fixe, le AP redémarre au lieu de se réinitialiser. Le voyant doit clignoter en orange.
3. Relâchez le bouton **Réinitialisation**.

   La configuration est réinitialisée aux paramètres par défaut. Lorsque la réinitialisation est terminée, le commutateur redémarre. Ce processus prend environ deux minutes.

   Avertissement: Pour éviter tout risque de corruption du micrologiciel, n'interrompez pas la réinitialisation. N'éteignez pas le PA. Patientez jusqu'à ce que le APredémarre et que le voyant s'allume en vert ou en bleu.

Utilisez l'interface utilisateur du périphérique pour réinitialiser le commutateur AP

Vous pouvez utiliser l'APinterface utilisateur du terminal de pour rétablir APles paramètres par défaut de.

ATTENTION: Ce processus efface tous les paramètres que vous avez configurés dans le routeur.

Pour rétablir les paramètres par défaut du commutateur à l'aide de l'interface utilisateur du périphérique :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > maintenance > Réinitialiser > restaurer les paramètres par défaut**.

   La page restaurer les paramètres par défaut s'affiche.
5. Cliquez sur le bouton **restaurer les paramètres par défaut**.

   Une fenêtre d'avertissement s'affiche.
6. Cliquez sur le bouton **Restore** (Restaurer).

Les fenêtres contextuelles se ferment et la configuration est réinitialisée aux paramètres par défaut. Lorsque la réinitialisation est terminée, le commutateur redémarre. Ce processus prend environ deux minutes.

Avertissement: Pour éviter tout risque de corruption du micrologiciel, n'interrompez pas la réinitialisation. Par exemple, ne fermez pas le navigateur, ne cliquez pas sur un lien et ne chargez pas de nouvelle page. N'éteignez pas le PA. Patientez jusqu'à ce que le APredémarre et que le voyant s'allume en vert ou en bleu.

Activez SNMP et gérez les paramètres SNMP

Vous pouvez accéder à AP via une connexion SNMP (simple Network Management Protocol), qui permet à un logiciel de gestion de réseau SNMP tel que HP OpenView de gérer APà l'aide du protocole v2 ou v3. Par défaut, SNMP est désactivé.

Pour activer SNMP et gérer les paramètres SNMP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > maintenance > gestion à distance** .

   La page gestion à distance s'affiche.

5. Sélectionnez l'option **Activer** SNMP.

   Par défaut, SNMP est désactivé.

   Vous pouvez maintenant configurer les paramètres SNMPv1/v2c et SNMPv3.

Configurez les paramètres SNMPv1/v2c

Vous pouvez configurer le paramètre SNMP v1/v2c après avoir activé SNMP sur le AP. Par défaut, SNMP est désactivé.

Pour activer SNMP et gérer les paramètres SNMPv1/v2c :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > maintenance > gestion à distance** .

   La page gestion à distance s'affiche.
5. Sélectionnez l'option **Activer** SNMP.

Par défaut, SNMP est désactivé.

6. Sélectionnez l'option **Activer** SNMP v1/v2c.
7. Dans la section SNMP v1/v2c, spécifiez les paramètres suivants :
   - **Nom de communauté en lecture seule** : Chaîne de communauté qui permet au gestionnaire SNMP de lire APles objets MIB du système . Le nom par défaut est snmpv1v2cuser.
   - **Nom de communauté trap** : Nom de communauté associé à l'adresse IP qui doit recevoir les interruptions. Par défaut, le bouton permettant d'utiliser le nom de communauté comme trappe est sélectionné. Pour créer un autre nom de recouvrement, désélectionnez la bascule **utiliser le même nom comme recouvrement**. Le nom de trapuser par défaut est défini sur trapuser.

   REMARQUE: Pour le nom de communauté en lecture seule et le nom de communauté de trap chacun, le nom peut comporter au maximum 30 caractères alphanumériques et spéciaux, à l'exception des guillemets (“) et des barres obliques inverses (\).
8. Dans la section interruption SNMP, spécifiez les paramètres suivants :
   - **Adresse IP (pour recevoir des interruptions)**: Adresse IP du gestionnaire SNMP qui doit recevoir des interruptions.
   - **Port de déroutement** : Numéro de port sur lequel le gestionnaire SNMP doit recevoir des interruptions. Le numéro par défaut est 162. La seule autre option est le numéro de port 161.
9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Configurez les paramètres SNMPv3.configurez les paramètres SNMPv3

Vous pouvez configurer le paramètre SNMP (simple Network Management Protocol) v3 après avoir activé SNMP sur le AP. Par défaut, SNMP est désactivé.

Pour activer SNMP et gérer les paramètres SNMP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > maintenance > gestion à distance** .

   La page gestion à distance s'affiche.

5. Sélectionnez l'option **Activer** SNMP.

   Par défaut, SNMP est désactivé.

6. Sélectionnez l'option **Activer** SNMP v3.

7. Dans la section SNMP v3, spécifiez les paramètres suivants :

   a. Dans le champ **nom d'utilisateur**, entrez un nom d'utilisateur pour SNMPv3. La valeur par défaut est snmpv3user.

   b. Dans le champ **phrase de passe d'autorisation**, saisissez une phrase de passe. Le mot de passe doit comporter entre 8 et 63 caractères et doit être une combinaison de caractères alphanumériques et spéciaux, à l'exception des

guillemets (") et d'une barre oblique inverse (\). La phrase de passe par défaut est snmp1234.

c. Dans le champ **phrase de passe priv**, saisissez une phrase de passe. Le mot de passe doit comporter entre 8 et 63 caractères et doit être une combinaison de caractères alphanumériques et spéciaux, à l'exception des guillemets (") et d'une barre oblique inverse (\). La phrase de passe par défaut est snmp1234.

d. Sélectionnez un niveau de sécurité dans le menu **niveau de sécurité** :

- **NoAuthNoPriv** : Pas d'authentification, pas de niveau de sécurité de confidentialité. Vous ne pouvez pas modifier les champs Protocole d'autorisation, phrase de passe d'autorisation, Protocole privé ou phrase de passe privée dans ce mode.
- **AuthNoPriv** : Niveau de sécurité authentification uniquement. Vous pouvez modifier les champs Protocole d'autorisation, phrase de passe d'autorisation, mais vous ne pouvez pas modifier les champs Protocole priv ou phrase de passe priv dans ce mode.
- **AuthPriv** : Niveau de sécurité de l'authentification et de la confidentialité. Vous pouvez modifier tous les champs.

e. Sélectionnez le protocole d'authentification dans le menu **Auth Protocol** :

- MD5 : Message Digest 5 (MD5) est le protocole d'authentification.
- **SHA** : Secure Hash Algorithm (SHA) est le protocole d'authentification. SHA offre une sécurité plus forte que MD5.

f. Sélectionnez le protocole privilégié dans le menu **Priv Protocol** :

- **DES** : SNMPv3 sont cryptés à l'aide du protocole de cryptage DES.
- AES Les paquets SNMPv3 sont chiffrés à l'aide du protocole AES, qui offre une sécurité plus forte que LES.

8. Facultatif : Par défaut, le bouton permettant d'utiliser le nom SNMPv3 comme trappe est sélectionné. Pour créer un autre nom de recouvrement, désélectionnez la bascule **utiliser le même nom comme recouvrement**. Le nom de trappe par défaut s'ajuste à snmptrap. Spécifiez les paramètres suivants :

a. Dans le champ **nom d'utilisateur**, entrez un nom d'utilisateur pour SNMPv3. La valeur par défaut est snmptrap.

b. Dans le champ **phrase de passe d'autorisation**, saisissez une phrase de passe. Le mot de passe doit comporter entre 8 et 63 caractères et doit être une combinaison de caractères alphanumériques et spéciaux, à l'exception des

guillemets (") et d'une barre oblique inverse (\). La phrase de passe par défaut est snmp1234.

c. Dans le champ **phrase de passe priv**, saisissez une phrase de passe. Le mot de passe doit comporter entre 8 et 63 caractères et doit être une combinaison de caractères alphanumériques et spéciaux, à l'exception des guillemets (") et d'une barre oblique inverse (\). La phrase de passe par défaut est snmp1234.

d. Sélectionnez un niveau de sécurité dans le menu **niveau de sécurité** :

- **NoAuthNoPriv** : Pas d'authentification, pas de niveau de sécurité de confidentialité. Vous ne pouvez pas modifier les champs Protocole d'autorisation, phrase de passe d'autorisation, Protocole privé ou phrase de passe privée dans ce mode.
- **AuthNoPriv** : Niveau de sécurité authentification uniquement. Vous pouvez modifier les champs Protocole d'autorisation, phrase de passe d'autorisation, mais vous ne pouvez pas modifier les champs Protocole priv ou phrase de passe priv dans ce mode.
- **AuthPriv** : Niveau de sécurité de l'authentification et de la confidentialité. Vous pouvez modifier tous les champs.

e. Sélectionnez le protocole d'authentification dans le menu **Auth Protocol** :

- MD5 : Message Digest 5 (MD5) est le protocole d'authentification.
- **SHA** : Secure Hash Algorithm (SHA) est le protocole d'authentification. SHA offre une sécurité plus forte que MD5.

f. Sélectionnez le protocole privilégié dans le menu **Priv Protocol** :

- **DES** : SNMPv3 sont cryptés à l'aide du protocole de cryptage DES.
- AES Les paquets SNMPv3 sont chiffrés à l'aide du protocole AES, qui offre une sécurité plus forte que LES.

9. Dans la section interruption SNMP, spécifiez les paramètres suivants :

- **Adresse IP (pour recevoir des interruptions)**: Adresse IP du gestionnaire SNMP qui doit recevoir des interruptions.
- **Port de déroutement** : Numéro de port sur lequel le gestionnaire SNMP doit recevoir des interruptions. Le numéro par défaut est 162. La seule autre option est le numéro de port 161.

10. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

Gérer la LED

Par défaut, la LED unique est activée et fonctionne comme décrit dans la section Voyants du panneau supérieur à la page 18. Vous pouvez déterminer si les LED s'allument ou non. Cette fonction est utile si vous souhaitez que le APfonctionne dans un environnement sombre.

Pour activer ou désactiver le voyant :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > contrôle LED** .

La page contrôle d'accès s'affiche.

5. Sélectionnez l'une des cases d'option suivantes :
   - **Activer la LED**: Le voyant est activé. Il s'agit de l'option par défaut.
   - **Désactiver la LED**: Le voyant est désactivé.
   - **Activer la LED pour les fonctions d'alimentation et de cloud** : Le voyant est activé pour les fonctions d'alimentation et de Cloud uniquement.
6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérer le mode efficacité énergétique

Si aucun client WiFi n'est connecté au AP, le AP peut automatiquement passer en mode d'efficacité énergétique (EEM) pour réduire la consommation d'énergie et économiser de l'énergie. Lorsqu'un ou plusieurs clients WiFi se connectent, le APquitte automatiquement l'EEM pour reprendre le fonctionnement normal.

Si EEM est activé et qu'aucun client WiFi n'est connecté au AP, le fonctionnement du flux d'antenne est limité à 1x1. (Dans des circonstances normales, le AP peut prendre en charge plusieurs flux d'antennes.) Si un client WiFi établit une connexion au AP, les flux d'antenne reprennent leur fonctionnement normal.

Notez les restrictions suivantes :

- Systèmes WDS (Wireless Distribution System) EEM s'exclut mutuellement avec un système de distribution sans fil (WDS, voir Configurez un pont WiFi dans un système de distribution sans fil à la page 341).
- Détection des points d'accès voisins EEM ne permet pas aux radios 5 GHz et 6 GHz de détecter les points d'accès voisins (voir Gérer la détection des points d'accès voisins à la page 147).
- **Canaux DFS** : Lorsque des clients WiFi se connectent au AP et que le AP reprend son fonctionnement normal, les transmissions radio 5 GHz peuvent être temporairement suspendues si le AP fonctionne sur un canal DFS (suspension d'environ 1 minute pour un canal DFS ; suspension d'environ 10 minutes pour un canal DFS météo).

REMARQUE: Si vous utilisez EEM, nous vous recommandons d'activer le guidage de bande sur vos réseaux WiFi. L'orientation de bande permet aux clients WiFi compatibles 5 GHz connectés à la bande 2,4 GHz d'être orientés vers la bande 5 GHz ou 6 GHz pour de meilleures performances. Pour plus d'informations, consultez la section Activer ou désactiver le guidage de bande à la page 103.

Pour activer ou désactiver le mode efficacité énergétique :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Configuration > système > Avancé > mode efficacité énergétique** .

   La page mode efficacité énergétique s'affiche.

5. Sélectionnez un bouton radio :
   - Activer. Le mode efficacité énergétique est activé.
   - Désactiver : Le mode efficacité énergétique est désactivé. Il s'agit de l'option par défaut.
6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Configurez le mode de puissance d'entrée PoE

Vous pouvez définir manuellement le niveau PoE utilisé parAP. En fonction de la quantité d'alimentation requise parAP, vous pouvez choisir un niveau d'alimentation spécifique dans l'interface utilisateur du terminal.

Pour configurer les paramètres d'alimentation du point d'accès :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > système > Avancé > Paramètres d'alimentation** .

   La page Paramètres d'alimentation s'affiche.

5. Dans le menu **mode**, sélectionnez l'un des paramètres d'alimentation suivants :

   - **Automatique** Le mode efficacité énergétique est activé. Il s'agit de l'option par défaut.
   - 802.3af : Il s'agit du paramètre de base PoE.
   - 802.3at : Il s'agit du paramètre PoE+.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre contextuelle s'affiche pour vous avertir d'un risque d'endommagement de l'équipement si la source PoE ne correspond pas au mode PoE sélectionné.

7. Pour continuer, cliquez sur **continuer**.

   Les paramètres sont enregistrés.

11

Surveillez le AP et le réseau

Ce chapitre décrit comment surveiller le APet le réseau.

Ce chapitre comprend les sections suivantes :

- Affiche les APparamètres Internet, IP et système
- Afficher les paramètres radio WiFi
- Afficher les points d'accès voisins inconnus et connus
- Afficher les statistiques des stratégies de trafic MAC et IP
- Afficher la distribution des clients, les clients connectés et les tendances des clients
- Échec DHCP de l'affichage
- Afficher le volume de trafic, les informations sur les ventilateurs, les statistiques et l'utilisation des canaux
- Afficher ou télécharger les URL suivies
- Affichez, enregistrez, téléchargez ou effacez les journaux
- Afficher une connexion de pont WiFi
- Afficher les alarmes et les notifications

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Affiche les APparamètres Internet, IP et système

Pour afficher les APparamètres de , Internet, IP et système :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Localisez le volet informations sur l'état de la connexion (généralement à gauche de la page), le volet informations sur le système (généralement au centre supérieur de la page) et le volet informations sur les paramètres IP (généralement au centre inférieur de la page).

Si la largeur de page de votre appareil est étroite, ces volets peuvent se trouver ailleurs sur le tableau de bord.

Pour plus d'informations sur le volet des paramètres radio (généralement à droite de la page), reportez-vous à la section Afficher les paramètres radio WiFi à la page 288.

Les paramètres suivants s'affichent :

- **Volet informations sur l'état de la connexion** : Ce volet se trouve dans le coin supérieur gauche du tableau de bord (si la largeur de la page sur votre appareil est suffisante ; sinon, il peut se trouver ailleurs) et affiche les éléments suivants :
  - État de la connexion à la plate-forme de gestion basée sur le cloud Netgear insight, le cas échéant
  - État de la connexion Internet
  - Mode de fonctionnement du AP, qui est toujours point d'accès
  - Nombre de périphériques connectés au AP
- **Volet informations système** : Ce volet se trouve au centre en haut du tableau de bord (si la largeur de page sur votre appareil est suffisante ; sinon, il peut se trouver ailleurs) et affiche les éléments suivants :
  - Nom du système APet pays ou région d'exploitation
  - Adresse MAC Ethernet
  - Le numéro de série
  - AP Durée de fonctionnement
  - Version du micrologiciel (firmware)
  - Date et heure auxquelles le APou quelqu'un a vérifié manuellement pour la dernière fois si un nouveau micrologiciel était disponible

  Ce volet contient également un bouton sur lequel vous pouvez cliquer pour rechercher les mises à jour du micrologiciel pour le AP. Si une mise à jour est disponible, l'écran Download Update Available (Télécharger la mise à jour disponible) s'ouvre. (Pour plus d'informations sur les mises à jour du micrologiciel, reportez-vous à la section Laissez le AP rechercher un nouveau micrologiciel et mettez-le à jour à la page 254).
- **Volet informations sur les paramètres IP** : Ce volet se trouve au centre du tableau de bord (si la largeur de la page sur votre appareil est suffisante ; sinon, il peut se trouver ailleurs) et affiche les éléments suivants :
  - Adresse IP du AP et son état DHCP
  - Adresse IP de la passerelle :

- État de la passerelle
- Volume du trafic filaire

5. Pour afficher des informations plus détaillées, sélectionnez **gestion > surveillance > système**.

   La page système s'affiche.

   La page affiche cinq sections :

   - **Section informations système** : Les paramètres suivants s'affichent :
     - **Nom du système** : APNom NetBIOS
     - **Mode système** : Le APmode système (AP)
     - Adresse MAC LAN Adresse MAC du port Ethernet LAN du AP
     - Adresse MAC sans fil pour 2,4 GHz Adresse MAC de l'interface WiFi (radio) 2,4 GHz du AP
     - Adresse MAC sans fil pour 5 GHz Adresse MAC de l'interface WiFi (radio) 5 GHz du AP
     - Adresse MAC sans fil pour 6 GHz Adresse MAC de l'interface WiFi (radio) 6 GHz du AP
     - Source d'alimentation Le type de source d'alimentation (niveau détecté d'alimentation PoE ou d'adaptateur secteur)

       Pour plus d'informations sur le niveau PoE, reportez-vous à la section Le AP fonctionne comme un PoE PD et le voyant clignote en vert en continu à la page 371.
     - LLDP Ethernet État de la fonction LLDP Ethernet (activé ou Désactivé)
     - **Voisin LLDP** : Voisin détecté par LLDP
     - Pays / région Le pays ou la région dans lequel APopère ou pour lequel est autorisé leAP
     - Version actuelle du firmware Version du micrologiciel exécutée sur le AP
     - **Version du micrologiciel de sauvegarde** : Version du micrologiciel de sauvegarde sur le AP
     - Version du Bootloader Version du chargeur d'amorçage principal (U-Boot) installée sur le AP
     - Numéro de série : Numéro de série du point d'accès AP

- Heure actuelle : Heure système actuelle du AP
- Durée de fonctionnement : Temps écoulé depuis le dernier redémarrage duAP

- **État de l'interface AP** : Une icône verte indique que l'interface est en cours d'utilisation. Une icône grise indique que l'interface n'est pas utilisée.
- **Section Paramètres IPv4** : Les paramètres suivants s'affichent :
  - Adresse IPv4 : Adresse IPv4 du AP
  - **Subnet Mask** (Masque de sous-réseau). Masque de sous-réseau du AP
  - Passerelle par défaut Passerelle par défaut pour AP
  - Client DHCP État du client DHCP (activé ou Désactivé)
- **Statut opérationnel du ventilateur** : Les paramètres suivants s'affichent :
  - **Température du système (°C)**: La température interne du APen degrés Celsius
  - **Régime du ventilateur** : Vitesse de rotation par minute (tr/min) du ventilateur interne
- **Section Paramètres sans fil** : Les paramètres suivants s'affichent, avec des colonnes distinctes pour les radios :
  - Antenne Le type d'antenne (par défaut, 2x2).
  - Mode Wifi Mode WiFi de la radio.
  - **Canal / fréquence**: Canal et fréquence utilisés par la radio.
  - **Puissance TX (en dBm)**: Puissance de transmission en dBm.

Afficher les paramètres radio WiFi

Pour afficher les paramètres radio WiFi du AP:

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations,

consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Localisez le volet informations radio dans le coin supérieur droit du tableau de bord (si la largeur de page de votre appareil est suffisante ; sinon, elle pourrait se trouver ailleurs).

   Les paramètres suivants s'affichent :

   - État de la radio (si l'icône 2,4 GHz, 5 GHz ou 6 GHz est grisée, la radio est désactivée).
   - Mode
   - Canal
   - Largeur du canal
   - Nombre de clients connectés et nombre maximal de clients pris en charge
   - Volume du trafic WiFi
   - Utilisation du canal
   - Antenne

5. Pour afficher des informations sur une autre radio, cliquez sur l'onglet **2,4 GHz**, **5 GHz** ou **6 GHz** .

   Le volet s'ajuste.

6. Pour afficher des informations plus détaillées, sélectionnez **gestion > surveillance > système**.

   La page système s'affiche.

   La page affiche cinq sections :

   - **Section informations système** : Les paramètres suivants s'affichent :
     - **Nom du système** : APNom NetBIOS
     - **Mode système** : Le APmode système (AP)
     - Adresse MAC LAN Adresse MAC du port Ethernet LAN du AP
     - Adresse MAC sans fil pour 2,4 GHz Adresse MAC de l'interface WiFi (radio) 2,4 GHz du AP
     - Adresse MAC sans fil pour 5 GHz Adresse MAC de l'interface WiFi (radio) 5 GHz du AP
     - Adresse MAC sans fil pour 6 GHz Adresse MAC de l'interface WiFi (radio) 6 GHz du AP
     - Source d'alimentation Le type de source d'alimentation (niveau détecté d'alimentation PoE ou d'adaptateur secteur)

       Pour plus d'informations sur le niveau PoE, reportez-vous à la section Le AP fonctionne comme un PoE PD et le voyant clignote en vert en continu à la page 371.
     - LLDP Ethernet État de la fonction LLDP Ethernet (activé ou Désactivé)
     - **Voisin LLDP** : Voisin détecté par LLDP
     - Pays / région Le pays ou la région dans lequel APopère ou pour lequel est autorisé leAP
     - Version actuelle du firmware Version du micrologiciel exécutée sur le AP
     - **Version du micrologiciel de sauvegarde** : Version du micrologiciel de sauvegarde sur le AP
     - Version du Bootloader Version du chargeur d'amorçage principal (U-Boot) installée sur le AP
     - Numéro de série : Numéro de série du point d'accès AP

  - Heure actuelle : Heure système actuelle du AP
  - Durée de fonctionnement : Temps écoulé depuis le dernier redémarrage duAP
- **État de l'interface AP** : Une icône verte indique que l'interface est en cours d'utilisation. Une icône grise indique que l'interface n'est pas utilisée.
- **Section Paramètres IPv4** : Les paramètres suivants s'affichent :
  - Adresse IPv4 : Adresse IPv4 du AP
  - **Subnet Mask** (Masque de sous-réseau). Masque de sous-réseau du AP
  - Passerelle par défaut Passerelle par défaut pour AP
  - Client DHCP État du client DHCP (activé ou Désactivé)
- **Statut opérationnel du ventilateur** : Les paramètres suivants s'affichent :
  - **Température du système (°C)**: La température interne du APen degrés Celsius
  - **Régime du ventilateur** : Vitesse de rotation par minute (tr/min) du ventilateur interne
- **Section Paramètres sans fil** : Les paramètres suivants s'affichent, avec des colonnes distinctes pour les radios :
  - Antenne Le type d'antenne (par défaut, 2x2).
  - Mode Wifi Mode WiFi de la radio.
  - **Canal / fréquence**: Canal et fréquence utilisés par la radio.
  - **Puissance TX (en dBm)**: Puissance de transmission en dBm.

Afficher les points d'accès voisins inconnus et connus

Si vous avez activé la détection des points d'accès voisins (voir Gérer la détection des points d'accès voisins à la page 147), vous pouvez afficher les points d'accès inconnus dans la liste des points d'accès inconnus et les points d'accès connus dans la liste des points d'accès connus.

Pour afficher les points d'accès voisins détectés :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > surveillance > AP voisin** .

   La page AP voisin s'affiche.

   En haut de la page, pour chaque bande radio, la page affiche le nombre total de points d'accès inconnus.

   Pour plus d'informations sur le déplacement des points d'accès inconnus vers la liste des points d'accès connus, reportez-vous à la section Activez la détection des points d'accès voisins et déplacez les points d'accès vers la liste des points d'accès connus à la page 148.

5. Pour afficher les points d'accès inconnus les plus récents, cliquez sur le bouton **Actualiser**.
6. Pour afficher la liste des points d'accès connus, cliquez sur l'onglet **points d'accès connus**.

   La page s'ajuste.

   En haut de la page, pour chaque bande radio, la page affiche le nombre total de points d'accès connus.
7. Pour afficher les points d'accès connus les plus récents, cliquez sur le bouton **Actualiser**.

Afficher les statistiques des stratégies de trafic MAC et IP

Vous pouvez afficher les statistiques de trafic pour les stratégies de trafic MAC et IP globales et spécifiques au SSID (règles de trafic). Pour chaque règle, ces statistiques comprennent le nombre de paquets et le nombre d'octets sur lesquels une règle a pris effet.

Pour afficher les statistiques de trafic, vous devez avoir activé les règles de trafic :

- Filtre antibruit sans fil Si vous activez le filtre anti-bruit sans fil (voir Activez ou désactivez le filtre antibruit sans fil à la page 160) et que vous activez une ou plusieurs règles de trafic globales (voir Activez, désactivez ou modifiez une règle de trafic dans le filtre antibruit sans fil à la page 161), vous pouvez afficher les statistiques de trafic associées au niveau MAC ou IP des règles de trafic.
- Filtre de trafic global Si vous activez le filtre de trafic global (voir Activez ou désactivez le filtre de trafic global à la page 168) et que vous ajoutez *et* activez une ou plusieurs règles de trafic global (voir Ajoutez une règle de trafic au filtre de trafic global à la page 169), vous pouvez afficher les statistiques de trafic associées au niveau MAC ou IP des règles de trafic.
- **Groupe spécifique au SSID** : Si vous activez au moins un groupe de filtres de trafic MAC/IP (voir Activer ou désactiver un groupe de filtres de trafic MAC/IP à la page 205), ajoutez *et* activez une ou plusieurs règles de trafic (voir Ajoutez une règle de trafic à un groupe de filtres de trafic MAC/IP à la page 207) et rattachez le groupe à un réseau WiFi (voir Sélectionnez un groupe de filtres de trafic MAC/IP pour un réseau WiFi à la page 332), vous pouvez afficher les statistiques de trafic associées au niveau MAC ou IP des règles de trafic.

Pour afficher les statistiques des stratégies de trafic MAC et IP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Pour afficher les statistiques de trafic, sélectionnez **gestion > surveillance > statistiques du filtre de trafic MAC/IP** .

   La page statistiques des filtres de trafic MAC/IP s'affiche.
5. Pour afficher les statistiques de trafic pour le filtre antibruit sans fil, dans la section groupes système, cliquez sur l'onglet **> filtre antibruit sans fil**. (L'onglet peut être sélectionné par défaut.)

   La page affiche les informations et statistiques suivantes pour chaque règle de trafic activée dans le filtre antibruit sans fil :

- **Priority** (Priorité). Ordre de priorité de la règle.
- Nom de la règle Nom de la règle.
- Action : Indique si le trafic est autorisé ou refusé.
- **Couche réseau** : Indique si la règle fonctionne au niveau MAC ou IP.
- Paquets Nombre de paquets sur lesquels la règle a pris effet.
- Octets Nombre d'octets sur lesquels la règle a pris effet.

6. Pour afficher les statistiques de trafic pour le filtre de trafic global, dans la section groupes à l'échelle du système, cliquez sur l'onglet **> filtre de trafic global**.

   La page affiche les informations et statistiques suivantes pour chaque règle de trafic activée dans le filtre de trafic global :

   - **Priority** (Priorité). Ordre de priorité de la règle.
   - Nom de la règle Nom de la règle.
   - Action : Indique si le trafic est autorisé ou refusé.
   - **Couche réseau** : Indique si la règle fonctionne au niveau MAC ou IP.
   - Paquets Nombre de paquets sur lesquels la règle a pris effet.
   - Octets Nombre d'octets sur lesquels la règle a pris effet.

7. Pour afficher les statistiques de trafic d'un groupe spécifique que vous avez associé à un réseau WiFi (SSID), dans la section groupes spécifiques au SSID, cliquez sur l'onglet **> Groupe** correspondant au numéro de groupe.

   La page affiche les informations et statistiques suivantes pour chaque règle de trafic activée dans le groupe :

   - **Priority** (Priorité). Ordre de priorité de la règle.
   - Nom de la règle Nom de la règle.
   - Action : Indique si le trafic est autorisé ou refusé.
   - **Couche réseau** : Indique si la règle fonctionne au niveau MAC ou IP.
   - Paquets Nombre de paquets sur lesquels la règle a pris effet.
   - Octets Nombre d'octets sur lesquels la règle a pris effet.

8. Pour afficher les informations les plus récentes, cliquez sur le bouton **Actualiser**.
9. Pour que la page s'actualise automatiquement, cliquez sur le bouton **actualisation automatique**.

Lorsque la page est configurée pour être actualisée automatiquement, le bouton actualisation automatique s'affiche en bleu et la page est actualisée toutes les 30 secondes.

10. Pour réinitialiser tous les compteurs, cliquez sur le bouton **Réinitialiser les compteurs**.

Afficher la distribution des clients, les clients connectés et les tendances des clients

Pour afficher les clients connectés au AP via WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Localisez le volet distribution client (généralement au milieu à gauche de la page) et le volet clients récents (généralement au milieu à droite de la page).

   Le volet distribution des clients affiche les types de clients (Windows, Mac, iOS, Android, Linux et autres systèmes d'exploitation) et la façon dont ces clients sont répartis sur les réseaux. (Par défaut, le bouton réseau est sélectionné.)

   Le volet clients récents affiche la liste des 5 principaux clients récemment connectés.

5. Pour afficher la répartition des clients sur les radios, cliquez sur le bouton **Radio** dans le volet distribution des clients.

   La page ajuste et affiche les types de clients pour chaque radio.

6. Pour afficher les clients récents pour tous les réseaux ou un seul réseau, dans le volet clients récents, cliquez sur l'icône de filtre et sélectionnez **tous les clients WiFi** ou les clients pour un réseau WiFi spécifique (SSID).

   Pour votre sélection, le volet affiche le nombre total de clients connectés et les noms de périphériques des clients connectés.

7. Pour afficher des informations sur un client connecté, cliquez sur son nom de périphérique.

   La page affiche l'adresse MAC, le type de périphérique, l'adresse IP et le SSID du client. Vous pouvez également afficher plus d'informations, y compris des informations très détaillées (voir Étape 11 et Étape 12).

8. Pour afficher les tendances relatives aux clients, faites défiler jusqu'au volet Hours Trend (tendance des heures) (généralement au bas de la page).

Le volet Hours Trend affiche un graphique indiquant le nombre de clients, le trafic en Mbit/s, l'utilisation du canal ou la condition du ventilateur sur une période que vous pouvez sélectionner.

Par défaut, les informations sur le client sont sélectionnées (c'est-à-dire que le bouton **Client** est sélectionné) et le graphique indique le nombre total de clients pour toutes les radios et le nombre de clients pour chaque radio (2,4 GHz, 5 GHz et 6 GHz).

Vous pouvez également cliquer sur le bouton **Traffic**, **Channel Utilization** ou **Fan**. Pour plus d'informations, consultez la section Afficher le volume de trafic, les informations sur les ventilateurs, les statistiques et l'utilisation des canaux à la page 302.

9. Pour afficher plus d'informations, pointez sur un nœud sur l'une des lignes du graphique.
10. Pour modifier la période pendant laquelle les informations sont filtrées et affichées, sélectionnez le nombre d'heures récentes dans le menu à droite des boutons.
11. Pour afficher plus d'informations sur les clients actuellement connectés, sélectionnez **gestion > surveillance > clients connectés** .

    La page Connected clients s'affiche.

    Pour chaque radio, la page affiche le nombre de clients connectés et le nombre maximal de clients pris en charge. Les clients connectés qui prennent en charge l'opération Multi-link (MLO) sont mis en surbrillance sous les radios partenaires sur la page.

    Pour chaque radio et chaque client WiFi, la page affiche le SSID, l'adresse MAC, l'adresse IP, le nom d'hôte (pour plus d'informations, reportez-vous à la section Attribuez des noms d'hôte aux clients WiFi et gérez la liste des noms d'hôte à la page 338), le système d'exploitation (OS), le mode WiFi, l'ID VLAN et le nom d'utilisateur ou l'identificateur de clé (pour une configuration multi-PSK).
12. Pour afficher des informations très détaillées sur un client WiFi, cliquez sur l'icône d'informations (i) à gauche du client.

    La page informations détaillées sur le client s'affiche et affiche les informations suivantes :

    - **MAC Address** (Adresse IP). Adresse MAC du client
    - **IP Address** (Adresse IP). Adresse IP associée au client.
    - Nom de l'hôte Nom d'hôte du client
    - OS Système d'exploitation exécuté sur le client.
    - BSSID BSSID auquel le client se connecte.
    - SSID : SSID de la radio à laquelle le client se connecte.

- Canal : Canal auquel le client se connecte.
- **Largeur du canal** Largeur du canal auquel le client se connecte.
- "Taux de transmission" Débit de transmission du trafic du client.
- "Taux de réception" Taux de réception du trafic du client.
- RSSI : Valeur de seuil RSSI du client.
- Octets de transmission Nombre d'octets transmis par le client.
- Octets de réception Nombre d'octets reçus par le client.
- **Paquets/octets unicast TX** : Nombre de paquets et d'octets de monodiffusion transmis par le client.
- **Paquets/octets unicast RX** : Nombre de paquets et d'octets de monodiffusion reçus par le client.
- **Paquets/octets de diffusion TX** : Nombre de paquets et d'octets de diffusion transmis par le client.
- **Paquets/octets multidiffusion TX** : Nombre de paquets et d'octets de multidiffusion transmis.
- **Erreurs/tentatives TX** : Nombre d'erreurs de transmission ou de tentatives effectuées en raison d'échecs de transmission.
- **Erreurs/tentatives Rx** : Nombre d'erreurs de réception ou de tentatives dues à la perte ou à la corruption de paquets.
- Etat : État QoS de la connexion.
- Type : Type de sécurité WiFi utilisé pour la connexion.
- Type d'appareil Type de périphérique du client.
- **Mode**: Le mode WiFi de la connexion.
- **MLO pris en charge**: Indique si le client prend en charge MLO.
- **MLD Address** (Adresse IP). Si le client prend en charge MLO, l'adresse MAC du périphérique à liaisons multiples (MLD).
- Etat : État de sécurité de la connexion.
- **Temps d'inactivité** : Durée pendant laquelle le client est resté inactif.
- **Horodatage associé** : Heure associée aux informations de la page informations détaillées sur le client.
- Identifiant VLAN : VLAN dans lequel le client est placé

- **Nom d'utilisateur/identificateur de clé** : Nom d'utilisateur ou identificateur de clé (pour une configuration Multi PSK) du client.
- **Soutien PMF** : Si PMF est activé sur le AP, indique si le client prend en charge PMF.

13. Si vous avez ouvert la page informations détaillées sur le client, cliquez sur le bouton **Fermer**.

    La page informations détaillées sur le client se ferme.

14. Pour afficher les statistiques des clients connectés sous forme graphique, cliquez sur l'icône graphique à droite du client.
    La page statistiques du client s'affiche avec les deux onglets suivants :
    - **Statistiques TX/Rx** : Vous pouvez afficher séparément les statistiques Unicast, Broadcast et Multicast. Vous pouvez choisir différentes périodes pour afficher les données historiques.
      - Cliquez sur le bouton **tous** pour afficher le trafic Tx et Rx pour les statistiques unicast, Broadcast et Multicast.
      - Cliquez sur le bouton **cumulatif Tx/Rx** pour afficher le total des paquets Tx et Rx (la somme des paquets Unicast, Broadcast et Multicast).
    - Utilisation du canal Vous pouvez afficher le pourcentage d'utilisation du canal pour chaque client. Vous pouvez choisir différentes périodes pour afficher les données historiques.
15. Pour actualiser les informations du graphique statistiques Tx/Rx ou utilisation du canal, cliquez sur le bouton **Actualiser**.
16. Pour réinitialiser les données statistiques client, cliquez sur le bouton **Réinitialiser les statistiques**.

Échec DHCP de l'affichage

Vous pouvez afficher les clients Wi-Fi qui n'ont pas terminé le processus DHCP DORA (découverte, offre, demande, accusé de réception) lors de la tentative de connexion au sur la page DHCP Failures (échecs DHCP)AP. Le processus DORA est utilisé pour attribuer une adresse IP à un client à partir du serveur DHCP.

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > surveillance > clients connectés > défaillances DHCP** .

   La page échecs DHCP s'affiche et affiche les informations suivantes :

   - Clients Affiche le nombre total de clients ayant échoué le processus DHCP.
   - Lignes par page : Permet de sélectionner le nombre d'entrées affichées sur une page. Vous pouvez choisir d'afficher 10, 25, 50, 100 ou 200 entrées à la fois.
   - Recherche : Utilisez la barre de recherche pour trouver des clients spécifiques en saisissant leur adresse MAC ou leur bande Wi-Fi.
   - **MAC Address** (Adresse IP). Affiche l'adresse MAC de chaque client ayant échoué le processus DHCP.
   - **bande** Affiche la bande Wi-Fi (2,4 GHz ou 5 GHz) sur laquelle la panne s'est produite.

- **Horodatage en échec** : Affiche la date et l'heure exactes auxquelles la panne DHCP s'est produite pour chaque client.
- Actions Affiche le bouton **chronologie**.
- **Refresh** (Actualiser). Cliquez sur le bouton **Actualiser** pour afficher les dernières informations sur l'échec DHCP du AP.

5. Pour afficher les dernières informations sur l'échec DHCP à partir de AP, cliquez sur le bouton **Actualiser** .
6. Cliquez sur le bouton **chronologie** dans la colonne actions pour ouvrir une fenêtre contextuelle chronologie de connexion détaillée. Cette fenêtre contextuelle fournit un résumé visuel de la chronologie du processus DORA :

   La chronologie du processus DORA affiche les quatre principales étapes du processus DHCP :

   - **Discover** : le client envoie une requête pour trouver un serveur DHCP.
   - **Offre** : Le serveur DHCP offre une adresse IP.
   - Demandes Le client demande l'adresse IP proposée.
   - **Accuser**réception : Le serveur DHCP confirme et attribue l'adresse IP.

   Problèmes courants : Répertorie les raisons possibles de l'échec.

   Par exemple : Offre DHCP non reçue.

   Réparation rapide : Fournit des suggestions pour aider à résoudre le problème.

   Par exemple :

   - L'offre DHCP n'a pas été reçue dans le délai imparti, probablement en raison d'une incompatibilité VLAN.
   - Vérifiez la configuration du port VLAN sur le commutateur et le routeur de liaison montante.

   MAC client et bande : Affiche l'adresse MAC et la bande du client en bas de la fenêtre contextuelle.

Afficher le volume de trafic, les informations sur les ventilateurs, les

statistiques et l'utilisation des canaux

Afficher le volume de trafic, les informations sur les ventilateurs, les statistiques et l'utilisation des canaux

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Faites défiler jusqu'au volet tendances des heures situé en bas du tableau de bord.

Par défaut, le bouton **clients** est sélectionné. Pour plus d'informations, consultez la section Afficher la distribution des clients, les clients connectés et les tendances des clients à la page 296.

5. Pour afficher les informations routières, procédez comme suit :
   a. Cliquez sur le bouton **trafic**.

      Le graphique présente les informations relatives au trafic Ethernet (LAN câblé), au trafic WiFi total, au trafic WiFi pour la radio 2,4 GHz, au trafic WiFi pour chaque radio 5 GHz et au trafic WiFi pour la radio 6 GHz.
   b. Pour afficher plus d'informations, pointez sur un nœud sur l'une des lignes du graphique.
6. Pour afficher l'utilisation du canal, procédez comme suit :
   a. Cliquez sur le bouton **Channel Utilization**.

      Le graphique montre l'utilisation du canal pour la radio 2,4 GHz.

      Le graphique affiche les pourcentages d'utilisation pour trois catégories :
      - Utilisation totale du canal : Utilisation globale du canal.
      - Utilisation de canal libre : Pourcentage d'utilisation du point d'accès actuel.
      - Utilisation du canal OBSS (chevauchement de l'ensemble de services de base) : Pourcentage d'utilisation des réseaux qui se chevauchent dans le même canal opérationnel.
   b. Pour afficher l'utilisation du canal d'une autre radio, cliquez sur le bouton **5 GHz** ou **6 GHz**.
   c. Pour afficher plus d'informations, pointez sur une barre.
7. Pour afficher les informations sur le ventilateur, procédez comme suit :
   a. Cliquez sur le bouton **ventilateur**.

      Le graphique indique la température du système et le régime du ventilateur.
   b. Pour afficher plus d'informations, pointez sur une barre.
8. Pour modifier la période pendant laquelle les informations sont filtrées et affichées, sélectionnez le nombre d'heures récentes dans le menu à droite des boutons.
9. Pour afficher les statistiques de trafic, sélectionnez **gestion > surveillance > statistiques**.

   La page statistiques s'affiche.

   La page Statistics fournit des informations détaillées sur les données de trafic du APdepuis le démarrage ou le redémarrage duAP :

- **Statistiques AP** : Cet onglet affiche le trafic globalAP
- **Statistiques radio** : Cet onglet affiche le trafic de chaque radio WiFi. Sélectionnez 2,4 GHz, 5 GHz ou 6 GHz GHz dans le menu déroulant pour afficher les statistiques de trafic de cette radio WiFi.
- **Statistiques SSID** : Cet onglet affiche les statistiques de trafic d'un SSID. Sélectionnez le nom du SSID dans le menu déroulant pour afficher les statistiques de trafic de ce SSID.
- **Statistiques WDS** : Cet onglet affiche le trafic lié au système de distribution sans fil (WDS). Sélectionnez le nom de l'interface WDS dans le menu déroulant pour afficher les statistiques de trafic de cette interface WDS.
- **Statistiques ARP** : Cet onglet affiche les statistiques de trafic ARP (Address Resolution Protocol), y compris le nombre de paquets proxy et abandonnés, si le proxy ARP est activé. Pour plus d'informations, consultez la section Gérer le proxy ARP à la page 359.
- **Statistiques Ethernet** : Cet onglet affiche le trafic de l'interface Ethernet.

Les statistiques de trafic s'affichent dans les formats suivants :

Représentation tabulaire : Vous pouvez afficher diverses statistiques de trafic sous forme de tableau.

Représentation graphique : Vous pouvez afficher APles statistiques de , Radio et SSID sous forme graphique.

- Vous pouvez afficher séparément les statistiques Unicast, Broadcast et Multicast.
- Cliquez sur le bouton **All Traffic** pour afficher le trafic Tx et Rx pour les statistiques Unicast, Broadcast et Multicast.
- Cliquez sur le bouton **cumulatif Tx/Rx** pour afficher le total des paquets Tx et Rx (la somme des paquets Unicast, Broadcast et Multicast).
- Vous pouvez choisir différentes périodes pour afficher les données historiques.

10. Pour actualiser les informations de la page, cliquez sur **le** bouton Actualiser.
11. Pour réinitialiser les informations de la page statistiques, cliquez sur le bouton **Réinitialiser les statistiques**.

Afficher ou télécharger les URL suivies

Si vous avez activé le suivi des URL pour un réseau WiFi (voir Activer ou désactiver le suivi d'URL pour un réseau WiFi à la page 320), vous pouvez afficher les URL suivies par URL, client WiFi et SSID. Vous pouvez également télécharger un rapport de suivi d'URL sous forme de fichier `.csv`.

Pour afficher ou télécharger des URL suivies :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > surveillance > suivi d'URL** .

   La page URL Tracking s'affiche.

   Par défaut, le tableau indique les URL auxquelles le client WiFi a accédé, chacune avec l'adresse MAC du client WiFi qui a accédé à l'URL, le SSID associé et le nombre de fois que le client WiFi a accédé à l'URL.

5. Pour afficher des informations supplémentaires, cliquez sur le bouton **...** Lien à droite d'une adresse MAC ou d'un SSID.
6. Pour afficher les informations de suivi d'URL par client WiFi, procédez comme suit :

   a. Dans le menu **liste par** , sélectionnez **Client**.

      Le tableau indique les adresses MAC des clients WiFi, chacune avec le nom d'hôte du client et la première URL de la liste des URL auxquelles le client a accédé.

   b. Pour afficher toutes les URL auxquelles un client WiFi a accédé, cliquez sur le bouton **...** Lien à droite de la première URL.

      Une fenêtre contextuelle affiche toutes les URL auxquelles le client WiFi a accédé.

   c. Cliquez sur le bouton **Fermer**.

      La fenêtre contextuelle se ferme.

7. Pour afficher les informations de suivi d'URL par SSID, procédez comme suit :

   a. Dans le menu **liste par** , sélectionnez **SSID**.

      Le tableau indique les SSID et la première URL de la liste des URL auxquelles le SSID a accédé.

   b. Pour afficher toutes les URL auxquelles vous avez accédé sur le SSID, cliquez sur le bouton **...** Lien à droite de la première URL.

      Une fenêtre contextuelle affiche toutes les URL auxquelles le système a accédé via le SSID.

   c. Cliquez sur le bouton **Fermer**.

      La fenêtre contextuelle se ferme.

8. Pour télécharger un rapport de suivi d'URL sous forme de fichier `.csv`, cliquez sur le bouton **Télécharger** et suivez les instructions de votre navigateur.
9. Pour afficher les informations les plus récentes, cliquez sur le bouton **Actualiser**.
10. Pour effacer toutes les informations de suivi d'URL, procédez comme suit :

    a. Cliquez sur le bouton **Clear** (Effacer).

Une fenêtre d'avertissement s'affiche.

b. Cliquez sur le bouton **OK** (Enregistrer).

La fenêtre contextuelle se ferme et les informations sont effacées.

Affichez, enregistrez, téléchargez ou effacez les journaux

Vous pouvez afficher et gérer les journaux d'activité du AP. Vous pouvez également télécharger un fichier journal détaillé.

REMARQUE: Si APfonctionne en mode de gestion Netgear insight, vous pouvez également afficher et gérer les journaux d'activité du cloud, qui indiquent la connexion de APà la plate-forme de gestion basée sur le cloud Insight. Si les AP fonctions du mode de gestion Netgear insight, cette option est disponible dans le tableau de bord en sélectionnant **gestion > surveillance > journaux Cloud** .

Pour afficher, enregistrer, télécharger ou effacer les journaux :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > surveillance > journaux**.

   La page journaux s'affiche, affichant tous les événements récents avec un horodatage.

5. Pour enregistrer les journaux, procédez comme suit :
   a. Cliquez sur le bouton **Save** (Enregistrer).
   b. Suivez les instructions de votre navigateur pour enregistrer le fichier sur votre ordinateur.
6. Pour télécharger les entrées de journal détaillées sous forme de fichier zip, procédez comme suit :
   a. Cliquez sur le bouton **Télécharger les journaux détaillés**.

      Selon la taille du fichier, le téléchargement des entrées de journal détaillées peut prendre plusieurs minutes.
   b. Suivez les instructions de votre navigateur pour enregistrer le fichier sur votre ordinateur.
7. Pour actualiser l'écran de connexion, cliquez sur le bouton **Refresh** (Actualiser).

   ATTENTION: Après avoir effacé les entrées du journal, vous ne pouvez plus les enregistrer ou les télécharger.
8. Pour effacer les entrées du journal, cliquez sur le bouton **Clear Log** (Effacer le journal).

Afficher une connexion de pont WiFi

Vous pouvez configurer un système de distribution sans fil (WDS) composé de connexions de pont WiFi point à point entre deux AP(voir Configurez un pont WiFi dans un système de distribution sans fil à la page 341). Ce réseau est différent d'un réseau WiFi maillé instantané Netgear insight.

Vous pouvez indiquer si un pont WiFi est établi et afficher la fonction (station de base ou répéteur), les adresses MAC et IP des APs qui forment le pont WiFi.

Pour afficher une connexion de pont WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > surveillance > Pont sans fil** .

   La page qui s'affiche vous permet de sélectionner un profil WDS (WDS 1, WDS 2, WDS 3 ou WDS 4).

5. Cliquez sur le bouton **>** à gauche d'un profil WDS.

   La page Pont sans fil s'affiche pour le profil WDS sélectionné.

6. Pour afficher la fonction, l'adresse MAC et l'adresse IP d'un AP, pointez sur AP.

Afficher les alarmes et les notifications

Vous pouvez afficher les alarmes et les notifications à partir de n'importe quelle AP page. La procédure suivante décrit comment les afficher à partir du tableau de bord.

Pour afficher les alarmes et les notifications :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Localisez l'icône de la sonnerie d'alarme en haut à droite de la page.

   L'icône affiche un nombre indiquant le nombre total de nouvelles alarmes et notifications depuis la dernière fois que vous avez affiché des alarmes et notifications.

5. Cliquez sur l'icône en forme de cloche d'alarme.

   La fenêtre contextuelle affiche les alarmes (signalées par une cloche rouge) et les notifications (signalées par une cloche bleue) avec une description et une heure.

6. Pour afficher plus d'alarmes et de notifications, faites défiler la fenêtre contextuelle vers le bas.

12

Gérer les fonctions WiFi avancées d'un réseau WiFi

Ce chapitre décrit comment gérer les fonctions WiFi avancées d'un réseau WiFi.

Pour plus d'informations sur les fonctions WiFi de base d'un réseau WiFi, reportez-vous à la section Gérer les fonctions WiFi de base d'un réseau WiFi à la page 71.

Ce chapitre comprend les sections suivantes :

- Définissez le mode NAT ou Bridge pour l'adressage et le trafic
- Activer ou désactiver l'isolation client pour un réseau WiFi
- Activer ou désactiver le suivi d'URL pour un réseau WiFi
- Sélectionnez une liste de contrôle d'accès MAC pour les clients WiFi dans un réseau WiFi
- Définissez des limites de débit de bande passante pour un réseau WiFi
- Modifier le format des messages d'offre DHCP dans un réseau WiFi
- Sélectionnez une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi dans un réseau WiFi
- Bloquez tout trafic de diffusion et de multidiffusion pour un réseau WiFi
- Sélectionnez un groupe de filtres de trafic MAC/IP pour un réseau WiFi
- Configurer la sélection avancée du débit pour un réseau WiFi
- Attribuez des noms d'hôte aux clients WiFi et gérez la liste des noms d'hôte

REMARQUE: Si vous souhaitez modifier les paramètres d'un réseau WiFi sur le AP, utilisez une connexion filaire pour éviter d'être déconnecté lorsque les nouveaux paramètres WiFi prennent effet.

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Définissez le mode NAT ou Bridge pour l'adressage et le trafic

Par défaut, le mode d'adressage et de trafic du AP est le mode Pont, ce qui signifie que les clients WiFi reçoivent des adresses IP d'un serveur DHCP (ou d'un routeur fonctionnant comme un serveur DHCP) de votre réseau. Il s'agit généralement du même serveur DHCP qui attribue une adresse IP au système AP lui-même.

Vous pouvez également définir le mode NAT, qui active le APserveur DHCP du pour les clients WiFi. APLe serveur DHCP du système attribue une adresse IP dans une plage différente de l'adresse IP du système AP lui-même.

Le mode NAT et les fonctionnalités suivantes s'excluent mutuellement :

- Dynamic VLAN (voir Configurez un réseau WiFi ouvert ou sécurisé à la page 73)
- Multi PSK (voir Configurez Multi PSK pour un réseau WiFi à la page 97)
- Passerelle mDNS (voir Gérer la passerelle DNS multicast à la page 235)
- Management VLAN autre que le VLAN 1 par défaut (voir Définissez le VLAN de gestion et de VLAN 802.1Q à la page 224)

REMARQUE: Le mode NAT n'est pas pris en charge en Inde.

Pour définir le mode NAT ou Bridge pour l'adressage et le trafic :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Dans le menu **adressage et trafic**, sélectionnez le mode adressage et trafic :

   REMARQUE: Cette option n'est pas prise en charge en Inde.

   - Bridge : Les clients WiFi reçoivent leurs adresses IP du serveur DHCP du même réseau que le AP. Il s'agit du mode par défaut.
   - NAT Les clients WiFi reçoivent leurs adresses IP d'un pool d'adresses DHCP privées sur le AP. Si vous sélectionnez ce mode, par défaut, l'adresse réseau WLAN est 172.31.4.0 et le masque de sous-réseau par défaut est 255.255.252.0. Cela signifie que les clients WiFi se voient attribuer une adresse IP comprise entre 172.31.4.2 et 172.31.7,254. L'adresse IP du serveur DNS par défaut pour le WLAN est 8,8.8,8, et la durée de bail par défaut est de 1440 minutes (24 heures).

     Pour modifier la plage par défaut du pool d'adresses DHCP, du serveur DNS par défaut, de la durée de bail ou de tous les paramètres NAT, procédez comme suit :

     a. Dans le champ **adresse réseau** , entrez une adresse réseau différente de celle du AP. Par exemple, si APl'adresse IP du système est comprise entre

192.168.0.1 et 192.168.0.254 (plage d'adresses IP courantes), entrez une adresse réseau différente de 192.168.0,0.

b. Dans le menu **masque de sous-réseau**, sélectionnez le masque de sous-réseau approprié à votre adresse réseau.

c. Dans le champ **DNS**, entrez l'adresse IP du serveur DNS que vous souhaitez utiliser. Cette adresse IP doit être différente de l'adresse réseau WLAN que vous avez définie à l'étape précédente.

d. Dans le champ **durée de location (en minutes)**, saisissez la durée de location appliquée aux clients WiFi.

   Le temps de location peut être de 5 à 43200 minutes.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer ou désactiver l'isolation client pour un réseau WiFi

Par défaut, l'isolation des clients est désactivée pour un réseau WiFi (SSID ou VAP), ce qui permet la communication entre les clients WiFi associés au même réseau WiFi ou à des réseaux WiFi différents sur le point d'accès. Pour plus de sécurité, vous pouvez activer l'isolation des clients afin que les clients associés au même réseau WiFi ou à des réseaux WiFi différents *ne puissent pas* communiquer entre eux, à l'exception de la communication sur Internet, qui reste possible.

L'isolation du client WiFi s'exclut mutuellement avec les fonctionnalités suivantes :

- Groupe de filtres de trafic MAC/IP (voir Sélectionnez un groupe de filtres de trafic MAC/IP pour un réseau WiFi à la page 332)
- Sécurité WPA2 entreprise et sécurité WPA3 entreprise utilisant un réseau VLAN dynamique (DVLAN, voir Configurez un réseau WiFi ouvert ou sécurisé à la page 73 et Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90)
- Clé pré-partagée multiple (PSK, voir Configurez Multi PSK pour un réseau WiFi à la page 97)
- Passerelle DNS multicast (mDNS) (voir Gérer la passerelle DNS multicast à la page 235)

- Blocage du trafic de diffusion et de multidiffusion (voir Bloquez tout trafic de diffusion et de multidiffusion pour un réseau WiFi à la page 330)
- Une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi (voir Sélectionnez une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi dans un réseau WiFi à la page 328)

Pour activer ou désactiver l'isolation client pour un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.
5. Cliquez sur le bouton **>** à gauche du SSID.

Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Sous isolation du client sans fil, sélectionnez l'un des boutons radio suivants :
   - Désactiver : L'isolation client est désactivée pour le réseau WiFi. Il s'agit de l'option par défaut.
   - Activer. L'isolation client est activée pour le réseau WiFi. Les cases à cocher suivantes s'affichent :

   Si vous sélectionnez le bouton radio **Activer**, une case à cocher s'affiche (voir l'étape suivante).

8. Si la case **autoriser l'accès aux périphériques répertoriés ci-dessous** s'affiche : Pour ajouter des périphériques réseau exempts d'isolement afin que les clients soient autorisés à les atteindre, procédez comme suit :

   a. Cochez la case **autoriser l'accès aux périphériques répertoriés ci-dessous**.

      Par défaut, cette case à cocher est désactivée.

      La liste d'autorisation s'affiche.

   b. Dans le champ à droite, saisissez jusqu'à 16 adresses IP statiques et noms de domaine des périphériques que les clients sont autorisés à atteindre via le réseau WiFi.

      Par exemple, vous pouvez saisir l'adresse IP statique ou le nom de domaine d'une imprimante réseau que vous souhaitez mettre à la disposition des clients WiFi. Un nom de domaine sur la liste d'autorisations doit être résolu en une adresse IP statique. Le nom peut comporter jusqu'à 255 caractères.

   c. Cliquez sur le bouton **déplacer**.

      Les adresses et les noms de domaine sont ajoutés à la liste d'autorisation.

   d. Pour supprimer une, plusieurs ou la totalité des adresses et des noms de domaine, cochez les cases individuelles ou **sélectionnez tout**, puis cliquez sur le bouton **Supprimer**.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Activer ou désactiver le suivi d'URL pour un réseau WiFi

Vous pouvez activer le AP pour suivre toutes les URL demandées par les clients WiFi connectés à un réseau WiFi (SSID ou VAP). Cette fonction est désactivée par défaut, mais vous pouvez l'activer.

Pour plus d'informations sur l'affichage des URL suivies par SSID ou par client WiFi, reportez-vous à la section Afficher ou télécharger les URL suivies à la page 306.

Pour activer ou désactiver le suivi d'URL pour un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Sous suivi d'URL, sélectionnez l'un des boutons radio suivants :
   - Activer. Le suivi d'URL est activé pour le réseau WiFi.
   - Désactiver : Le suivi d'URL est désactivé pour le réseau WiFi.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Sélectionnez une liste de contrôle d'accès MAC pour les clients WiFi dans un réseau WiFi

Après avoir configuré une ou plusieurs listes de contrôle d'accès MAC locales (ACL, également appelées listes d'accès ; voir Gérer les listes de contrôle d'accès MAC pour les clients WiFi à la page 190), vous pouvez sélectionner une ACL à utiliser avec un SSID.

Selon la stratégie que vous avez définie pour une liste de contrôle d'accès, les périphériques WiFi dont l'adresse MAC figure sur la liste de contrôle d'accès MAC sont autorisés à accéder à AP via ce SSID ou refusés à l'accès au SSID. Si l'accès au SSID est refusé, ces périphériques peuvent se connecter à APvia un autre SSID si vous n'avez pas configuré la sécurité ACL MAC pour ce SSID.

Vous pouvez également configurer un serveur RADIUS (voir Configurer les serveurs RADIUS à la page 143) et sélectionner l'ACL MAC RADIUS. Vous devez définir l'ACL sur le serveur RADIUS, en utilisant le format suivant pour les adresses MAC des clients dans le serveur RADIUS : Si l'adresse MAC du client est 00:0a:95:9d:68:16, spécifiez-la comme 000a959d6816 dans le serveur RADIUS.

REMARQUE: Une ACL MAC RADIUS ne peut pas fonctionner si la sécurité WiFi est WPA2 entreprise ou WPA3 entreprise. Si vous souhaitez utiliser une liste de contrôle d'accès MAC RADIUS, sélectionnez un autre type de sécurité WiFi pour le réseau WiFi (voir Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90).

Avant de sélectionner une ACL MAC pour un réseau WiFi, consultez la politique de l'ACL :

- **Politique ACL autorisant l'accès**: Un périphérique WiFi sur la liste de contrôle d'accès est autorisé à accéder au SSID tandis que tous les autres périphériques WiFi se voient refuser l'accès au SSID.
- **Politique ACL refusant l'accès**: L'accès au SSID est refusé à un périphérique WiFi sur la liste de contrôle d'accès tandis que tous les autres périphériques WiFi sont autorisés à accéder au SSID.

Pour sélectionner une liste de contrôle d'accès MAC pour les clients WiFi dans un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Cochez la case **Activer le ACL**.
8. Effectuez l'une des opérations suivantes :

   - Sélectionnez le bouton radio **local MAC ACL** et, dans le menu **Select Group**, sélectionnez la MAC ACL que vous avez définie précédemment.

     Pour modifier la stratégie MAC ACL, les adresses MAC dans la liste ACL, ou les deux, cliquez sur le lien en regard du groupe. Pour plus d'informations, consultez la section Gérer les listes de contrôle d'accès MAC pour les clients WiFi à la page 190.

   - Sélectionnez le bouton radio **Radius MAC ACL**.

     Cette option ne fonctionne que si vous configurez un serveur RADIUS (voir Configurer les serveurs RADIUS à la page 143).

ATTENTION: Si vous accédez à l'interface utilisateur du terminal APvia une connexion WiFi, assurez-vous que votre terminal est autorisé à accéder au SSID. Sinon, votre terminal se verra refuser l'accès à l'interface utilisateur du terminal après que vous aurez cliqué sur le bouton **appliquer**.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Définissez des limites de débit de bande passante pour un réseau WiFi

Vous pouvez définir des limites de débit pour les bandes passantes de chargement et de téléchargement pour les appareils connectés à un réseau WiFi. Le débit de bande passante minimum est de 64 Kbit/s, le débit de bande passante maximum est de 1024 Mbit/s. Vous pouvez définir un débit pour la bande passante de téléchargement et un autre débit pour la bande passante de téléchargement.

REMARQUE: Vous pouvez définir des limites de débit de bande passante pour un maximum de deux réseaux WiFi sur le AP.

Pour définir des limites de débit de bande passante pour les appareils connectés à un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

- **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

  REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.
5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.
6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.
7. Cochez la case **Rate Limit**.
8. Spécifiez les valeurs :
   - Chargement : Pour la limite de bande passante de téléchargement, entrez une valeur comprise entre 64 et 1024 et sélectionnez **Kbps** ou **Mbps** dans le menu.
   - Téléchargement : Pour la limite de bande passante de téléchargement, entrez une valeur comprise entre 64 et 1024 et sélectionnez **Kbps** ou **Mbps** dans le menu.
9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Modifier le format des messages d'offre DHCP dans un réseau WiFi

Lorsqu'un terminal tente de s'associer au réseau WiFi et négocie une adresse IP, APconvertit le message d'offre DHCP de diffusion qu'il reçoit du serveur DHCP en message de monodiffusion, puis le transfère au terminal. Il s'agit de la configuration par défaut. Pour l'échange de messages DHCP, les paquets unicast sont plus fiables et minimisent le trafic sur le réseau.

Si votre situation exige que les messages d'offre DHCP soient distribués sous forme de paquets de diffusion dans un réseau WiFi spécifique, vous pouvez modifier le format de message pour ce réseau WiFi afin que le AP*ne* convertisse *pas* les messages d'offre DHCP de diffusion en messages monodiffusion.

Pour modifier le format des messages d'offre DHCP dans un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**

   La page qui s'affiche vous permet de sélectionner un SSID.
5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.
6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.
7. Faites défiler l'écran et cliquez sur l'onglet **> Traffic Policy**.

   La page se développe.
8. Sous DHCP Offer Broadcast to Unicast, sélectionnez l'un des boutons radio suivants :
   - Activer. Le APDHCP de transfert offre des messages sous forme de paquets unicast sur le réseau WiFi. Il s'agit de la sélection par défaut.
   - **Désactiver**. Le APserveur DHCP transfère les messages sous forme de paquets de diffusion sur le réseau WiFi.
9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Sélectionnez une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi dans un réseau WiFi

Après avoir configuré une ou plusieurs listes de contrôle d'accès MAC locales (ACL, également appelées listes d'accès) pour le trafic de diffusion et de multidiffusion à partir de clients WiFi, vous pouvez sélectionner une ACL à utiliser avec un SSID. Pour plus d'informations sur la configuration des listes de contrôle d'accès pour le trafic de diffusion et de multidiffusion des clients WiFi, reportez-vous à la section Listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi à la page 198.

Par défaut, tous les appareils WiFi sont autorisés à envoyer du trafic de diffusion et de multidiffusion vers un réseau WiFi. Si vous autorisez le trafic uniquement à partir de périphériques spécifiés et que vous sélectionnez une ACL, celle-ci fonctionne comme suit :

- Un périphérique WiFi pour lequel vous placez l'adresse MAC dans la liste de contrôle d'accès est autorisé à envoyer du trafic de diffusion et de multidiffusion au réseau WiFi.

  Le trafic de diffusion et de multidiffusion est autorisé dans le même SSID sur lequel le client WiFi envoie le trafic, quelle que soit la radio sur laquelle le SSID est diffusé. Si un autre SSID utilise le même VLAN, les clients de l'autre SSID peuvent également recevoir le trafic de diffusion ou de multidiffusion.

  Par exemple :

  - Le SSID du « lobby principal » utilise VLAN 1 et diffuse sur la radio 2,4 GHz et la radio 5 GHz.
  - L'adresse MAC du client 1 se trouve sur la liste de contrôle d'accès MAC et le client 1 envoie le trafic de multidiffusion sur la radio 5 GHz du SSID du « lobby principal ».
  - Le SSID « Auditorium » est également configuré sur le même VLAN 1 et diffuse sur la radio 2,4 GHz.
  - Le SSID « Service comptabilité » est configuré sur VLAN 2 et diffuse sur la radio 2,4 GHz et la radio 5 GHz.

  Dans ce cas, le trafic multicast du client 1 peut atteindre tous les clients connectés au SSID du « lobby principal » ainsi que tous les clients connectés au SSID de «

l’auditorium », mais il ne peut pas atteindre les clients connectés au SSID du « département comptable ».

- Le trafic de diffusion et de multidiffusion provenant de tous les autres appareils WiFi est rejeté par le réseau WiFi.

Pour sélectionner une liste de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion à partir de clients WiFi sur un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.
5. Cliquez sur le bouton **>** à gauche du SSID.

Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Faites défiler l'écran et cliquez sur l'onglet **> Traffic Policy**.

   La page se développe.

   Par défaut, la case autoriser le trafic de diffusion/multidiffusion est cochée.

8. Sélectionnez le bouton radio **autoriser le trafic uniquement à partir de périphériques spécifiés**.

9. Dans le menu **Groupe de périphériques autorisés**, sélectionnez la liste de contrôle d'accès MAC que vous avez définie précédemment.

   Pour modifier les adresses MAC dans la liste de contrôle d'accès, cliquez sur le lien **modifier le groupe** en regard du menu. Pour plus d'informations, consultez la section Listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi à la page 198.

10. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

Bloquez tout trafic de diffusion et de multidiffusion pour un réseau WiFi

Par défaut, le trafic de diffusion et de multidiffusion provenant de n'importe quel appareil peut atteindre un réseau WiFi. Vous pouvez également bloquer tout le trafic broadcast et multicast sur un réseau WiFi.

Pour bloquer tout le trafic de diffusion et de multidiffusion sur un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations,

consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l'appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s'affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Faites défiler l'écran et cliquez sur l'onglet **> Traffic Policy**.

   La page se développe.

   Par défaut, la case autoriser le trafic de diffusion/multidiffusion est cochée.

8. Désactivez la case à cocher **autoriser le trafic de diffusion/multidiffusion**.

9. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Le trafic haut débit et multicast n'est pas autorisé à atteindre le réseau WiFi.

Sélectionnez un groupe de filtres de trafic MAC/IP pour un réseau WiFi

Après avoir activé un groupe de filtre de trafic MAC/IP et ajouté une ou plusieurs règles de trafic au groupe, vous pouvez sélectionner le groupe à utiliser avec un réseau WiFi (SSID). Selon les paramètres des règles de trafic du groupe, les règles de trafic s'appliquent alors au trafic entrant, sortant ou entrant et sortant dans le SSID.

Pour plus d'informations sur la configuration du groupe filtre de trafic MAC/IP, reportez-vous à la section Gérer les groupes de filtres de trafic MAC/IP pour les réseaux WiFi à la page 205.

REMARQUE: Si vous appliquez un groupe de filtre de trafic MAC/IP à un réseau WiFi, le débit peut être affecté et peut être inférieur à la normale.

Pour sélectionner un groupe de filtres de trafic MAC/IP pour un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **> Avancé**.

   La page se développe.

7. Faites défiler l'écran et cliquez sur l'onglet **> Traffic Policy**.

   La page se développe.

8. Cochez la case **filtres de trafic MAC/IP**.

9. Dans le menu **sélectionner un groupe**, sélectionnez un groupe que vous avez défini précédemment.

   Pour modifier les règles de trafic dans le groupe, cliquez sur le lien **modifier le groupe** en regard du menu. Pour plus d'informations, consultez la section Gérer les groupes de filtres de trafic MAC/IP pour les réseaux WiFi à la page 205.

10. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

Configurer la sélection avancée du débit pour un réseau WiFi

La sélection avancée du débit vous permet d'améliorer la capacité d'un réseau WiFi *individuel* (par opposition à une radio, qui affecte *tous les* réseaux WiFi de la radio) afin d'atteindre l'équilibre optimal entre les composants suivants du réseau WiFi :

- Types de trafic (multidiffusion, gestion, contrôle et trafic de données)
- Nombre et proximité des clients (densité de clients)
- Types de clients (modes WiFi pris en charge par les clients, y compris les modes WiFi existants)
- Débit pour les clients
- Zone que le réseau WiFi doit couvrir

Pour configurer correctement la sélection avancée du débit, nous vous recommandons de déterminer ce que les clients de votre réseau peuvent avoir besoin (types de trafic, modes WiFi pris en charge et vitesse de débit attendue), combien de clients peuvent se connecter simultanément au réseau WiFi et où les clients peuvent se trouver.

REMARQUE: Par défaut, la sélection avancée du tarif est désactivée. Si vous activez la sélection avancée du débit, le AP applique les paramètres de contrôle du débit aux connexions WiFi d'un réseau WiFi standard, mais pas aux connexions d'un système de distribution sans fil (WDS) ou d'un réseau WiFi à maillage instantané Insight.

La sélection avancée du débit vous permet de configurer les paramètres suivants pour les bandes radio 2,4 GHz et 5 GHz dans un réseau WiFi (cette fonction ne s'applique pas à la bande radio 6 GHz) :

- Débit de multidiffusion fixe : Le taux de transmission du trafic multicast que vous sélectionnez est automatiquement appliqué. Les débits que vous pouvez sélectionner sont les débits de multidiffusion de base pris en charge par la bande radio.
- Contrôle du débit : Le débit que vous sélectionnez est automatiquement appliqué à la balise et aux autres trames de gestion, ainsi qu'aux trames de contrôle et de données. Si vous activez le contrôle de débit, vous pouvez définir le niveau de densité, qui se compose de quatre composants décrits ci-dessous. En d'autres termes, le niveau de densité comprend bien plus que la densité du client (le nombre et la proximité des clients dans le réseau WiFi).

  Les paramètres disponibles pour le niveau de densité dans le réseau WiFi dépendent du mode WiFi dans lequel la radio fonctionne. (Pour plus d'informations sur les

modes WiFi, reportez-vous à la section Permet de modifier le mode préambule d'une radio à la page 114.)

Vous pouvez définir un niveau de densité de 0 (en fait de 0 à 4, paramètre par défaut), 1 (de 1 à 4), 2 (de 2 à 4), 3 (de 3 à 4) ou 4. Le paramètre est ensuite appliqué aux composants *interdépendants* suivants, que vous ne pouvez pas définir individuellement précisément car ils sont interdépendants :

- **Densité**: Densité (nombre et proximité) des clients dans le réseau WiFi. (La densité est l'une des quatre composantes du *niveau* de densité .) Une valeur de 0 signifie une densité de clients très faible. Un réglage de 4 signifie une densité de clients très élevée.
- Compatibilité Compatibilité avec les modes WiFi pour les clients hérités du réseau WiFi. Pour la radio 2,4 GHz, un paramètre de 0 signifie la compatibilité avec les clients 802.11b/g/n/ax ; Un paramètre de 4 signifie la compatibilité avec les clients 802.11g/n/ax mais pas avec les clients 802.11b hérités.
- **Performance globale** : Débit des clients du réseau WiFi. Une valeur de 0 signifie une performance réduite. Un réglage de 4 signifie une performance optimale. Par exemple, vous pouvez délibérément sélectionner une performance réduite si vous avez besoin d'une zone de couverture très large.
- Couverture : Zone que le réseau WiFi doit couvrir. Un réglage de 0 signifie une zone de couverture très large. Un réglage de 4 signifie une zone de couverture très étroite. Par exemple, vous pouvez délibérément sélectionner une zone très étroite si vous avez besoin d'une performance optimale.

Une autre façon de décrire le niveau de densité est qu'un niveau sélectionné est mappé sur un niveau de densité client correspondant, le mode WiFi, le débit hérité minimum, le débit de balise et le débit MCS (modulation Coding Scheme) minimum.

Pour configurer la sélection avancée du débit pour un réseau WiFi :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

- **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

  REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **Gestion > Configuration > Wifi > Base > Paramètres WLAN**.

   La page qui s'affiche vous permet de sélectionner et d'ajouter un SSID.

5. Cliquez sur le bouton **>** à gauche du SSID.

   Les paramètres du SSID sélectionné s'affichent.

6. Faites défiler vers le bas et cliquez sur l'onglet **Advanced Rate Selection**.

   La page ajuste et affiche les paramètres de sélection de débit pour les bandes radio 2,4 GHz et 5 GHz.

   REMARQUE: Pour le SSID sélectionné, vous pouvez spécifier les paramètres radio pour les bandes radio 2,4 GHz et 5 GHz individuellement. Les descriptions des étapes suivantes s'appliquent aux deux radios.

7. Pour appliquer des débits de multidiffusion fixes de base, dans le menu **débit de multidiffusion fixe**, sélectionnez l'un des débits suivants, en fonction de la bande radio :

   - 2,4 GHz **1**, **2**, **5,5** ou **11** Mbit/s ou **Auto** (réglage par défaut).
   - 5 GHz **6**, **12** ou **24** Mbit/s ou **Auto** (réglage par défaut).

8. Pour activer le contrôle automatique du débit minimum pour les balises et autres trames de gestion ainsi que pour les trames de contrôle et de données, cochez la case **contrôle du débit**.

Si vous cochez la case **contrôle de débit**, le curseur **niveau de densité** devient disponible.

9. Pour définir le niveau de densité de votre environnement, déplacez le curseur **niveau de densité** sur **0**, **1**, **2**, **3** ou **4**.

   Lorsque vous déplacez le curseur, le niveau de densité sélectionné est mappé sur un mode WiFi, un débit de balise, un débit hérité minimum et un débit MCS minimum correspondants. Les paramètres disponibles dépendent du mode WiFi sélectionné pour la radio (voir Permet de modifier le mode préambule d'une radio à la page 114). Par défaut, le mode WiFi de chaque radio est 11ax.

   Le niveau de densité du réseau WiFi est basé sur les composants interdépendants suivants, pour lesquels un paramètre est affecté par la position du curseur mais *que vous ne pouvez pas définir individuellement*:

   - **Densité des clients WiFi** : Dans le mode WiFi 11ax par défaut pour les radios, le paramètre peut être très bas, faible, moyen, élevé ou très élevé, selon la position du curseur.
   - **Compatibilité avec les modes WiFi pour les clients hérités** : Dans le mode WiFi 11ax par défaut pour les radios, ce paramètre peut être le suivant :
     - 2,4 GHz Le paramètre 802.11b/g/n/ax, qui prend en charge les clients 802.11b, ou le paramètre 802.11g/n/ax, qui ne prend pas en charge les clients 802.11b.
     - 5 GHz Le paramètre 802.11a/n/AC/ax/Be, qui prend en charge tous les types de clients dans la bande radio 5 GHz dans n'importe quelle position du curseur.
   - **Performances globales pour les clients WiFi** : Dans le mode WiFi 11ax par défaut pour les radios, le paramètre peut être réduit, modéré, bon, très bon ou optimal, selon la position du curseur.
   - Couverture WiFi Dans le mode WiFi 11ax par défaut pour les radios, le paramètre peut être très étroit, étroit, moyen, large ou très large, selon la position du curseur.

   REMARQUE: Le texte d'aide de l'interface utilisateur du terminal fournit un tableau contenant des informations détaillées sur la façon dont le mode WiFi d'une radio affecte ces composants et sur la façon dont ces composants dépendent les uns des autres.

10. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

Attribuez des noms d'hôte aux clients WiFi et gérez la liste des noms d'hôte

Vous pouvez attribuer manuellement des noms d'hôte aux clients WiFi pour faciliter l'identification. Le AP peut prendre en charge un maximum de 600 entrées de nom d'hôte.

Vous devez connaître l'adresse MAC du client WiFi pour lequel vous souhaitez ajouter un nom d'hôte. L'adresse MAC peut s'afficher sur la page Connected clients (clients connectés) (voir Afficher la distribution des clients, les clients connectés et les tendances des clients à la page 296).

REMARQUE: Vous ne pouvez pas attribuer de nom d'hôte à une adresse MAC aléatoire.

Pour attribuer des noms d'hôte aux clients WiFi et gérer la liste des noms d'hôte :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sans fil > remplacement du nom d'hôte**.

   La page remplacement du nom d'hôte s'affiche.
5. Pour ajouter manuellement un nom d'hôte pour un client WiFi, procédez comme suit dans les champs situés sous la liste des noms d'hôte des clients :
   a. Dans le champ de gauche, saisissez ou copiez l'adresse MAC du client au format 1-00-00-00-00-00.
   b. Dans le champ **Entrez un nom d'hôte**, saisissez un nom pour le client. Le nom d'hôte doit contenir des caractères alphanumériques, peut contenir des tirets et ne peut pas dépasser 32 caractères. Le nom d'hôte ne peut pas commencer ou se terminer par un tiret.
   c. Pour ajouter un autre nom d'hôte, répétez les deux sous-étapes précédentes.

      Vous pouvez ajouter un maximum de 10 noms d'hôte à la fois.
   d. Cliquez sur le bouton **Add** (Ajouter).

      Les paramètres sont enregistrés.
6. Pour modifier un nom d'hôte, procédez comme suit dans la liste des noms d'hôte client :
   a. Cochez les cases correspondant au contenu.
   b. Cliquez sur le bouton **Modifier**.
   c. Modifiez le nom d'hôte.
   d. Pour modifier un autre nom d'hôte, répétez les trois sous-étapes précédentes.

Vous pouvez modifier jusqu'à 10 noms d'hôte à la fois.

e. Cliquez sur le bouton **Apply** (Appliquer).

Les paramètres sont enregistrés.

7. Pour supprimer un ou plusieurs noms d'hôte, procédez comme suit dans la liste des noms d'hôte client :

a. Cochez les cases correspondant au contenu.

Vous pouvez supprimer jusqu'à 10 noms d'hôte à la fois.

b. Cliquez sur le bouton **Supprimer**.

Les noms d'hôte sont supprimés.

13

Configurez un pont WiFi dans un système de distribution sans fil

Ce chapitre décrit comment configurer un système de distribution sans fil (WDS) composé de connexions de pont WiFi point à point entre deux APs. chaque connexion de pont WiFi nécessite un profil WDS pour lequel les paramètres doivent correspondre sur les APs qui composent le pont.

Un WDS *n'*est *pas* identique à un réseau WiFi Netgear insight instant Mesh, qui nécessite l'utilisation de Netgear insight et d'un point d'accès pour fonctionner en tant que racine (voir Installez le AP sur un réseau WiFi maillé instantané Insight à la page 58).

Ce chapitre comprend les sections suivantes :

- Exigences relatives à la station de base Wi-Fi, au répéteur Wi-Fi et au pont Wi-Fi
- Configurez un pont WiFi entre les points d'accès

REMARQUE: Si vous activez le mode efficacité énergétique, vous ne pouvez pas utiliser de WDS. Pour utiliser un WDS, désactivez d'abord le mode efficacité énergétique. Pour plus d'informations, consultez la section Gérer le mode efficacité énergétique à la page 280.

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Exigences relatives à la station de base Wi-Fi, au répéteur Wi-Fi et au pont Wi-Fi

Si le AP est connecté à Internet via une connexion filaire, le AP peut fonctionner comme station de base WiFi pour quatre autres APs au maximum qui fonctionnent comme répéteurs WiFi. Le APpeut également fonctionner comme un répéteur WiFi s'il est connecté à un autre AP qui fonctionne comme une station de base WiFi.

Une borne d'accès WiFi se connecte à Internet, les clients filaires et WiFi peuvent se connecter à la borne d'accès, et la borne d'accès envoie son signal WiFi à un ou plusieurs APrépéteurs WiFi. Les clients filaires et WiFi peuvent également se connecter à un répéteur WiFi, mais le répéteur se connecte à Internet via la borne d'accès WiFi.

La figure suivante montre deux APs dans une configuration de répétition WiFi avec une station de base WiFi sur le côté gauche et un seul répéteur WiFi sur le côté droit.

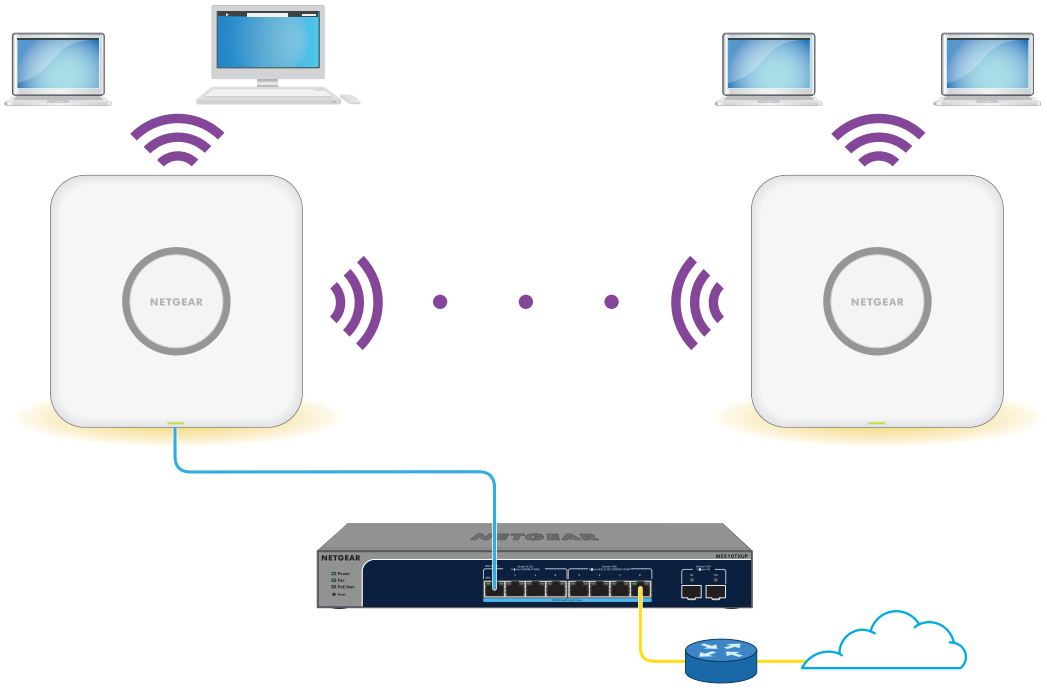

Illustration 8 : Configuration du pont WiFi entre deux APs dans la bande radio 5 GHz

Pour utiliser un pont WiFi, vous ne pouvez pas utiliser la fonction de canal automatique pour le AP et la diffusion SSID doit être activée.

Pour un pont WiFi, vous devez en configurer un AP comme station de base WiFi et un autre AP comme répéteur WiFi :

- **Station de base WiFi** : La station de base est connectée via Ethernet à un commutateur réseau (généralement avec une connexion Internet) et ponte le trafic vers et depuis le répéteur. La station de base gère également le trafic WiFi et câblé local. Pour configurer ce mode, vous devez connaître l'adresse MAC de la radio 2,4 GHz, 5 GHz ou 6 GHz sur le répéteur.
- Répéteur Wifi Le répéteur envoie tout le trafic de ses périphériques WiFi ou filaires locaux à la station de base WiFi. De même, le répéteur reçoit tout le trafic de ses ordinateurs WiFi ou filaires locaux de la station de base. Le répéteur est connecté au réseau (et à Internet) via la connexion WiFi à la station de base. Pour configurer ce mode, vous devez connaître l'adresse MAC de la radio 2,4 GHz, 5 GHz ou 6 GHz sur la station de base.

Avant de pouvoir configurer un réseau WiFi avec WDS, votre configuration doit remplir les conditions suivantes :

- Les deux APdoivent utiliser le même canal WiFi et les mêmes paramètres de sécurité WiFi.
- Les deux APdoivent se trouver sur le même sous-réseau IP LAN. Autrement dit, toutes les APadresses IP LAN se trouvent sur le même réseau.
- Tous les périphériques LAN (ordinateurs câblés et WiFi) sont configurés pour fonctionner dans la même plage d'adresses réseau LAN que lesAP

REMARQUE: Si vous utilisez le AP comme station de base avec un point d'accès non NETGEAR comme répéteur, vous devrez peut-être modifier d'autres paramètres de configuration. En particulier, vous devrez peut-être désactiver la fonction de serveur DHCP sur le point d'accès non NETGEAR qui est le répéteur.

ATTENTION: Avant de configurer un pont WiFi entre deuxAP, activez le protocole STP sur les AP(voir Activer ou désactiver le protocole Spanning Tree à la page 227) et sur les commutateurs auxquels les APsont connectés. Si vos commutateurs ne prennent pas en charge le protocole STP, une fois le pont WiFi établi, déconnectez l'un des APde son commutateur pour éviter les problèmes de boucle réseau et de connectivité. Si vous avez utilisé un commutateur PoE+ pour cela AP, vous devez maintenant utiliser un adaptateur secteur.

Configurez un pont WiFi entre les points d'accès

La procédure suivante décrit comment configurer les paramètres du pont WiFi sur l'un d'APentre eux, puis en faire de même sur l'autre AP, ce qui permet d'établir le pont WiFi.

Pour configurer un pont WiFi entre deux APs :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > Pont sans fil** .

   La page qui s'affiche vous permet de sélectionner un profil WDS (WDS 1, WDS 2, WDS 3 ou WDS 4).

5. Cliquez sur le bouton **>** à gauche d'un profil WDS.

   La page du profil WDS s'affiche.

6. Sélectionnez le bouton radio Band **2,4 GHz**, **5 GHz** ou **6 GHz** .

   Votre sélection détermine la bande radio sur laquelle le WDS est établi. Dans les pays qui ne prennent pas en charge le fonctionnement bi-bande ou tri-bande, vous ne pouvez pas sélectionner la radio.

7. Appuyez sur la case d'option d'agrégation VAP.

   Par défaut, un profil WDS est désactivé.

8. Sélectionnez l'un des boutons WDS-Role Selection suivants :

   - **Auto**. Le PAV WDS avec l'adresse MAC la plus élevée est la station de base et l'autre est le répéteur. Il s'agit de l'option par défaut.
   - **Station Arlo**. Le WDS VAP est la station de base WiFi.
   - Répéteur Le WDS VAP est le répéteur WiFi.

9. Configurez les paramètres du profil WDS comme décrit dans le tableau suivant.

Paramètre	Description
Nom du réseau sans fil (SSID)	Nom du réseau WiFi du réseau sur lequel le WDS est établi. Le nom par défaut est NETGEAR-WDS-x, où x est le numéro du WDS (1, 2, 3 ou 4). Le nom WiFi peut contenir jusqu'à 32 caractères et ne peut pas contenir de barre oblique inverse ni de guillemets doubles. **Remarque** : Le nom du réseau WiFi doit être identique sur la borne d'accès WiFi et le répéteur WiFi.
Adresse MAC locale	Adresse MAC de l'interface radio WDS locale, c'est-à-dire l'adresse MAC de la radio locale sur laquelle le WDS est établi. Vous ne pouvez pas modifier cette adresse MAC sur cette page. L'adresse MAC est affichée à titre indicatif. Entrez cette adresse MAC sur la connexion distante AP du WDS. **Remarque** : L'adresse MAC locale doit être différente de l'adresse MAC distante.

(A continué)

Paramètre	Description
Adresse MAC distante	Adresse MAC de l'interface radio WDS distante, c'est-à-dire l'adresse MAC de la radio distante sur laquelle le WDS est établi. **Remarque** : L'adresse MAC distante doit être différente de l'adresse MAC locale.
Authentification réseau, Chiffrement de données et Phrase d'authentification :	Si vous configurez le WDS sur la radio 2,4 GHz ou 5 GHz, la sélection par défaut dans le menu est ouvrir, auquel cas l'authentification et le cryptage des données ne sont pas applicables. Pour sécuriser la connexion WDS, sélectionnez **WPA2 personnel**. Si vous configurez le WDS sur la radio 6 GHz, la seule sélection par défaut du menu est WPA3 personnel. Pour la sécurité WPA personnel ou WPA3 personnel, spécifiez les paramètres suivants : • Chiffrement Le cryptage des données est AES et vous ne pouvez pas modifier ce paramètre. • Phrase d'authentification : Phrase secrète pour la connexion WDS. La phrase de passe peut contenir entre 8 et 63 caractères. Pour que vous puissiez activer la connexion WDS, la phrase de passe sur le serveur distant AP doit correspondre à la phrase de passe que vous avez définie dans ce champ.

10. Cliquez sur le bouton **Apply** (Appliquer).

    Les paramètres sont enregistrés.

11. Configurez les paramètres du pont WiFi sur le AP à l'autre extrémité du pont WiFi et redémarrez-le AP.

    REMARQUE: Si l'appareil situé à l'autre extrémité du pont WiFi est un point d'accès NETGEAR, vous n'avez peut-être pas besoin de le redémarrer.

    Le pont WiFi est établi.

12. Vérifiez la connectivité sur les réseaux locaux des deux APs..

    Si la configuration est correctement configurée, un ordinateur sur n'importe quel segment WiFi ou LAN câblé du AP qui fonctionne comme répéteur WiFi peut se connecter à Internet ou partager des fichiers et des imprimantes avec n'importe quel autre ordinateur ou serveur connecté au APqui fonctionne comme station de base WiFi.

REMARQUE: Une fois le pont WiFi établi, vous ne pouvez pas modifier le canal WiFi de la radio sur laquelle le pont WiFi est établi.

14

Gérer les fonctions avancées de la radio

Ce chapitre décrit comment gérer les fonctions radio avancées du AP. Pour plus d'informations sur les fonctions de base de la radio, reportez-vous à la section Gérer les fonctions de base de la radio à la page 107.

ATTENTION: Si vous modifiez une fonction radio sur la radio 2,4 GHz, la modification affecte tous les réseaux WiFi diffusant sur la radio 2,4 GHz. De même, si vous modifiez une fonction radio sur la radio 5 GHz ou 6 GHz, la modification affecte tous les réseaux WiFi diffusant sur la radio 5 GHz ou 6 GHz. Si la modification n'est pas spécifique à une radio, elle affecte *tous les* réseaux WiFi sur le AP.

Ce chapitre comprend les sections suivantes :

- Gérez les paramètres WiFi avancés des radios
- Gérer le nombre maximal de clients pour une radio
- Permet de gérer les paramètres de diffusion et de multidiffusion d'une radio
- Gérer l'équilibrage de charge des radios
- Gérez les clients collants
- Gérer le proxy ARP

REMARQUE: si vous souhaitez modifier les paramètres WiFi du routeur, utilisez une connexion filaire pour éviter d'être déconnecté lorsque les nouveaux paramètres WiFi prennent effet.

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Gérez les paramètres WiFi avancés des radios

Les paramètres WiFi avancés des radios s'appliquent à tous les réseaux WiFi (VPN ou SSID). Bien que ces paramètres fonctionnent correctement pour la plupart des environnements réseau et qu'il soit peu probable que vous ayez besoin de les modifier, vous *pouvez* modifier les paramètres radio, et vous pouvez le faire pour les radios 2,4 GHz, 5 GHz et 6 GHz individuellement.

ATTENTION: Nous vous recommandons de modifier ces paramètres WiFi avancés uniquement si vous en comprenez parfaitement les conséquences. Une configuration incorrecte peut entraîner des problèmes de connectivité pour les terminaux essayant de se connecter à AP.

Une radio doit être allumée pour que vous puissiez modifier les paramètres. Pour plus d'informations sur l'activation d'une radio, reportez-vous à la section Permet d'allumer ou d'éteindre une radio à la page 113.

Pour gérer les paramètres WiFi avancés des radios :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez Configuration > Wireless > Advanced > Wireless Settings (Configuration > Sans fil > Avancé > Paramètres sans fil).

   La page Paramètres sans fil pour les paramètres avancés s'affiche.

5. Spécifiez les paramètres comme décrit dans le tableau suivant.

   Les descriptions du tableau s'appliquent à toutes les radios. Vous pouvez spécifier les paramètres radio pour les radios 2,4 GHz, 5 GHz ou 6 GHz individuellement, mais la case à cocher de la fonction 802.11n 256 QAM s'applique uniquement à la radio 2,4 GHz (la fonction est toujours activée pour les radios 5 GHz et 6 GHz)) .

Paramètre	Description
Clients sans fil max	Saisissez le nombre maximal de clients WiFi pouvant être associés simultanément à la radio. Pour chaque radio, la plage est comprise entre 1 et 200 clients WiFi, et la valeur par défaut est 200.
Seuil RTS (256-2346)	Entrez le seuil de demande d'envoi (RTS). La plage est de 256 à 2346. Le numéro par défaut est 2346. Si la taille du paquet est inférieure ou égale au seuil RTS, la radio utilise le mécanisme CSMA/CD (Carrier Sense multiple Access with collision Detection) et la trame de données est transmise immédiatement après la période de silence. Si la taille du paquet est supérieure au seuil RTS, le système utilise le mécanisme CSMA avec évitement de collision (CSMA/CA). Dans cette situation, le dispositif émetteur envoie le paquet RTS au dispositif récepteur et attend que le dispositif récepteur renvoie un paquet CTS (Clear to Send) avant d'envoyer les données du paquet réel.
Intervalle de balise (100-300)	Entrez un intervalle compris entre 100 ms et 300 ms pour chaque transmission de balise, ce qui permet à la radio de synchroniser le réseau WiFi. La valeur par défaut est 100 ms. **Remarque** : Si vous configurez plus de quatre réseaux WiFi, l'intervalle de balise passe automatiquement à 300.

(A continué)

Paramètre	Description
802.11n 256 QAM	Lorsque le mode WiFi est 802.11n, vous pouvez cocher la case **802.11n 256 QAM** pour permettre à la radio 2,4 GHz de fonctionner sur une modulation d'amplitude en quadrature 256 (QAM), ce qui peut augmenter le débit radio 2,4 GHz pour les clients 802.11n prenant en charge 256 QAM. Par défaut, 256 QAM est activé pour la radio 2,4 GHz, c'est-à-dire que la case est cochée. Par défaut, 256-QAM est activé pour la radio 5 GHz et vous ne pouvez pas le désactiver (la page ne fournit pas de case à cocher pour la radio 5 GHz). La radio 6 GHz utilise une QAM plus élevée (la page ne contient pas de case à cocher pour la radio 6 GHz).
Intervalle DTIM (1-255)	Déplacez le curseur pour spécifier l'intervalle DTIM (Delivery Traffic indication message) ou le débit de balise de données, qui indique la période du message d'indication de trafic de livraison par balise en multiples intervalles de balise. Cette valeur doit être comprise entre 1 et 255. Le numéro par défaut est 3.
Limitation du débit de diffusion/multidiffusion	La limitation du débit de multidiffusion et de diffusion est activée par défaut pour améliorer les performances globales du réseau en limitant le nombre de paquets transmis sur le réseau. Par défaut, le paramètre est 64, ce qui spécifie une limite de débit maximale de 64 paquets par seconde. La limite est comprise entre 1 et 512 paquets par seconde. Pour modifier le paramètre, déplacez le curseur. Pour désactiver la multidiffusion et la limitation du débit de diffusion, décochez la petite case.
MU-MIMO	Par défaut, le bouton radio **Activer** MU-MIMO est sélectionné et la fonction MIMO multi-utilisateur (MU-MIMO) est activée. Pour désactiver MU-MIMO, sélectionnez le bouton radio **désactiver** MU-MIMO. La technologie MU-MIMO permet à plusieurs utilisateurs de recevoir simultanément des données du APen utilisant le même canal. Avec MU-MIMO, le AP peut transmettre simultanément à plusieurs clients en utilisant le même canal. La technologie MU-MIMO est utilisée en aval et nécessite que le AP et les clients WiFi prennent en charge la norme 802.11ac Wave 2 ou 802.11ax.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Gérer le nombre maximal de clients pour une radio

Le nombre de clients autorisés à s'associer à une radio affecte la fiabilité et le débit de la connexion WiFi. Un nombre plus petit peut augmenter la fiabilité et le débit et un nombre plus grand peut diminuer la fiabilité et le débit.

Par défaut, chaque radio autorise jusqu'à 200 associations de clients. Vous pouvez spécifier un nombre inférieur de clients. Si le nombre de clients associés dépasse le nombre maximal spécifié, la radio rejette les nouvelles associations de clients jusqu'à ce que le nombre tombe en dessous de ce nombre maximal.

Pour gérer le nombre maximal de clients pour une radio :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez Configuration > Wireless > Advanced > Wireless Settings (Configuration > Sans fil > Avancé > Paramètres sans fil).

   La page Paramètres sans fil pour les paramètres avancés s'affiche.

5. Dans le champ **Max.Wireless clients de** la radio, entrez le nombre maximal de clients WiFi pouvant être associés simultanément à la radio.

   La plage est comprise entre 1 et 200 clients WiFi, et la valeur par défaut est 200.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Une fenêtre d'avertissement s'affiche.

7. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Permet de gérer les paramètres de diffusion et de multidiffusion d'une radio

Étant donné que le trafic de multidiffusion et de diffusion peut affecter négativement le débit et la latence d'un réseau WiFi, vous pouvez modifier les paramètres de limitation du débit de multidiffusion et de diffusion d'une radio.

Par défaut, la limitation du débit de multidiffusion et de diffusion est activée pour améliorer les performances globales du réseau en limitant le nombre de paquets transmis sur le réseau. Par défaut, le paramètre est 64, ce qui spécifie une limite de débit maximale de 64 paquets par seconde. La limite est comprise entre 1 et 512 paquets par seconde.

Pour gérer les paramètres de diffusion et de multidiffusion d'une radio :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez Configuration > Wireless > Advanced > Wireless Settings (Configuration > Sans fil > Avancé > Paramètres sans fil).

   La page Paramètres sans fil pour les paramètres avancés s'affiche.

5. Pour modifier le paramètre de limitation du débit de multidiffusion et de diffusion d'une radio, déplacez le curseur **limitation du débit de diffusion/multidiffusion**.

   Par défaut, le paramètre est 64, ce qui spécifie une limite de débit maximale de 64 paquets par seconde. La limite est comprise entre 1 et 512 paquets par seconde.

6. Pour désactiver ou activer la limitation du débit de multidiffusion et de diffusion pour une radio, décochez ou cochez la case **limitation du débit de diffusion/multidiffusion**.

7. Cliquez sur le bouton **Apply** (Appliquer).

Une fenêtre d'avertissement s'affiche.

8. Cliquez sur le bouton **OK** (Enregistrer).

   La fenêtre contextuelle se ferme et vos paramètres sont enregistrés. La ou les radios redémarrent et les clients WiFi devront peut-être se reconnecter.

Gérer l'équilibrage de charge des radios

Vous pouvez configurer les seuils d'utilisation de la radio pour permettre à chaque radio de maintenir la vitesse et les performances du réseau WiFi lorsque les clients s'associent au réseau WiFi et s'en dissocient.

Si vous activez l'équilibrage de charge, les associations de clients dépendent du nombre maximal de clients par radio, de la charge de canal par radio et de l'indicateur de puissance du signal reçu (RSSI) de chaque client. Les associations de nouveaux clients sont autorisées si l'utilisation d'une radio reste dans les paramètres d'équilibrage de charge définis. Si l'utilisation d'une radio dépasse les paramètres d'équilibrage de charge définis, les associations de nouveaux clients sont temporairement interrompues jusqu'à ce que l'utilisation de la radio tombe dans les paramètres d'équilibrage de charge définis.

REMARQUE: Le tableau de bord peut afficher des informations sur le client et la distribution du trafic par radio, ainsi que sur le client, le trafic et l'utilisation des canaux pour chaque radio (voir Afficher la distribution des clients, les clients connectés et les tendances des clients à la page 296 et Afficher le volume de trafic, les informations sur les ventilateurs, les statistiques et l'utilisation des canaux à la page 302).

Par défaut, tous les types d'équilibrage de charge suivants sont activés avec leurs paramètres par défaut :

- **Équilibrage de charge basé sur le nombre maximum de clients**: Le système AP autorise les associations de clients jusqu'au nombre maximal spécifié de clients. Une fois le nombre maximum dépassé, les nouveaux clients sont rejetés. Même s'il s'agit d'un paramètre global, il est mis en œuvre par radio.
- **Équilibrage de charge basé sur la charge du canal** : Le système AP autorise les associations de clients jusqu'à l'utilisation maximale du canal définie. Lorsque l'utilisation maximale du canal est dépassée, les nouveaux clients sont rejetés. Même s'il s'agit d'un paramètre global, il est mis en œuvre par radio.

REMARQUE: Si un client est rejeté mais tente de manière persistante de s'associer à AP, le système AP accorde l'accès à ce client.

- **Équilibrage de charge basé sur le RSSI du client**: Les clients dont le RSSI est égal ou supérieur au minimum défini sont autorisés à s'associer au AP. Les clients dont le RSSI est inférieur au minimum défini sont rejetés. Même s'il s'agit d'un paramètre global, il est mis en œuvre par radio.

  REMARQUE: Si un client est rejeté mais tente de manière persistante de s'associer à AP, le système AP accorde l'accès à ce client.

Vous pouvez modifier les paramètres par défaut de chaque type d'équilibrage de charge ou désactiver complètement un ou plusieurs types d'équilibrage de charge.

Pour gérer l'équilibrage de charge des radios :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sans fil > Avancé > équilibrage de charge**.

   La page Load Balancing s'affiche.

5. Pour activer globalement l'équilibrage de charge pour les radios, sélectionnez le bouton radio **Activer** le mode d'équilibrage de charge.

   La page ajuste et affiche un curseur pour chaque type d'équilibrage de charge et chaque radio.

   Par défaut, l'équilibrage de charge est désactivé. Lorsque vous activez l'équilibrage de charge, les trois types d'équilibrage de charge sont activés. Vous pouvez désactiver individuellement un ou plusieurs types d'équilibrage de charge.

6. Pour activer ou désactiver individuellement un ou plusieurs types d'équilibrage de charge, procédez comme suit :
   - Pour désactiver un type particulier d'équilibrage de charge, décochez la petite case bleue à gauche du texte *basé sur ...*.
   - Pour activer un type particulier d'équilibrage de charge, cochez la petite case bleue à gauche du texte *basé sur ...*.

7. Pour modifier les paramètres d'équilibrage de charge, procédez comme suit :
   - **Basé sur le nombre maximum de clients**: Pour chaque radio, déplacez le curseur associé pour spécifier le nombre maximal de clients autorisés, avant que la radio cesse d'accepter de nouvelles associations de clients.

     Pour chaque radio, le nombre minimum de clients est 5, le nombre maximum est 200, et le nombre par défaut est 200.
   - **Basé sur la charge de canal** : Pour chaque radio, déplacez le curseur associé pour spécifier le pourcentage maximal de charge de canal autorisé sur la radio, avant qu'elle ne cesse d'accepter de nouvelles associations de clients.

     Pour chaque radio, le pourcentage minimum de charge de canal est de 50, le pourcentage maximum est de 90 et le pourcentage par défaut est de 70.
   - **Basé sur la puissance du signal de réception du canal** : Pour chaque radio, déplacez le curseur associé pour spécifier la valeur RSSI minimale requise pour un client individuel, en dessous de laquelle la radio n'accepte pas l'association client.

Pour chaque radio, la valeur RSSI minimale est 1, la valeur maximale est 50 et la valeur par défaut est 23.

8. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérez les clients collants

Pendant le Roaming, les clients persistants ne passent pas à un point d'accès avec un meilleur signal, mais restent associés (c'est-à-dire, *collent à*) à leur point d'accès initial, même si la qualité de la connexion à ce point d'accès est dégradée. Une telle situation entraîne un retard pour les autres clients associés à ce point d'accès.

REMARQUE: Pour un réseau WiFi domestique avec un seul point d'accès, un client rémanent est utile car aucun autre point d'accès n'est disponible pour être associé pendant le Roaming. Dans le cas d'un réseau d'entreprise ou d'entreprise comportant plusieurs points d'accès, un client inactif peut entraîner une consommation de ressources WiFi.

Vous pouvez forcer les clients rémanents à se dissocier des radios du AP.

Si l'équilibrage de charge basé sur le RSSI du client est activé (voir Gérer l'équilibrage de charge des radios à la page 354), une fois qu'un client est forcé de se dissocier, le client peut à nouveau se joindre dans les situations suivantes :

- Le client peut s'associer à nouveau si son RSSI est égal ou supérieur au RSSI minimum requis.
- Si le client tente en permanence de s'associer au système AP, le système AP accorde l'accès à ce client, même si son RSSI est inférieur au RSSI minimum requis.

Pour gérer les clients persistants :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sans fil > Avancé > équilibrage de charge**.
   La page Load Balancing s'affiche.

5. Activez ou désactivez la case à cocher **forcer les clients rémanents à se dissocier** :
   - **Les clients collants sont forcés de dissocier**: Cochez la case. Si la valeur RSSI d'un client est inférieure à la valeur RSSI minimale requise que vous avez définie pour une radio, le client est dissocié de force.

     Pour chaque radio, vous pouvez déplacer le curseur **basé sur la puissance du signal de réception du canal** pour spécifier la valeur RSSI minimale requise pour un client individuel, en dessous de laquelle la radio n'accepte pas l'association client.

Pour chaque radio, la valeur RSSI minimale est 1, la valeur maximale est 50 et la valeur par défaut est 23.

- **Les clients collants sont autorisés à rester associés**: Désactivez la case à cocher. Il s'agit de l'option par défaut.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

Gérer le proxy ARP

Par défaut, le proxy ARP est activé sur le AP, ce qui lui permet d'inspecter tous les paquets de diffusion ARP pour ses clients. De cette manière, le AP répond aux demandes ARP de ses clients, empêchant ainsi le trafic de diffusion inutile sur les radios.

Pour plus d'informations sur les statistiques ARP, y compris le nombre de paquets mandatés et abandonnés, reportez-vous à la section Afficher le volume de trafic, les informations sur les ventilateurs, les statistiques et l'utilisation des canaux à la page 302.

Pour gérer le proxy ARP :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Configuration > sans fil > Avancé > Proxy ARP** .

   La page Proxy ARP s'affiche.

5. Sélectionnez l'une des cases d'option suivantes :
   - Activer. Le proxy ARP est activé. Il s'agit de l'option par défaut.
   - Désactiver : Le proxy ARP est désactivé. Le trafic de diffusion sur les radios peut augmenter.

6. Cliquez sur le bouton **Apply** (Appliquer).

   Les paramètres sont enregistrés.

15

Diagnostics et dépannage

Ce chapitre décrit comment capturer des paquets WiFi et dépanner le APréseau et.

Ce chapitre comprend les sections suivantes :

- Capturez les paquets WiFi et Ethernet
- Effectuez un test ping
- Effectuez un test de débit
- Conseils rapides pour le dépannage WiFi
- Dépanner avec les voyants
- Le nœud et la racine ne peuvent pas se connecter
- Dépannez la connectivité WiFi pour un client WiFi
- Dépannage de la navigation Internet
- Vous ne pouvez pas vous connecter à APvia une connexion LAN
- Les modifications ne sont pas enregistrées
- Vous entrez un mot de passe incorrect et ne pouvez plus vous connecter à AP
- Dépannez votre réseau à l'aide de l'utilitaire ping

REMARQUE: Dans ce manuel, *réseau WiFi* signifie la même chose que SSID (identifiant de l'ensemble de services ou nom du réseau WiFi) ou VAP (point d'accès virtuel). Autrement dit, lorsque nous faisons référence à un réseau WiFi, nous entendons un SSID individuel ou VAP.

Capturez les paquets WiFi et Ethernet

Vous pouvez capturer les paquets WiFi et Ethernet reçus et transmis par le AP et enregistrer le fichier avec les paquets capturés sur votre ordinateur. Pendant le processus de capture de paquets, le fonctionnement normal du AP n'est pas affecté.

La capacité de capture de trames peut être utile pour analyser un déploiement WiFi, surveiller un réseau WiFi, déboguer des protocoles, déterminer les goulots d'étranglement du réseau WiFi et, en général, dépanner les irrégularités d'un réseau WiFi.

Vous pouvez choisir de capturer tous les paquets ou uniquement les paquets sélectionnés. Vous pouvez sélectionner une interface pont, une interface Ethernet ou des interfaces WLAN (radio 0 - 2,4 GHz / radio 1 - 5 GHz / radio 2 - 6 GHz) pour capturer les paquets.

REMARQUE: Pour afficher les paquets capturés, vous avez besoin d'une application capable d'ouvrir les fichiers `.pcap`.

Pour capturer des paquets :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Diagnostics > Packet Capture**.

   La page Capture de paquets s'affiche.

5. Spécifiez les paramètres comme décrit dans le tableau suivant.

Paramètre	Description
Interface de capture	Dans le menu **Capture interface**, sélectionnez l'une des interfaces suivantes sur lesquelles les paquets doivent être capturés : • **br-lan**. Tous les paquets sont capturés, c'est-à-dire les paquets sur les interfaces Ethernet, radio 2,4 GHz, radio 5 GHz et radio 6 GHz. • eth0 : Les paquets sur l'interface Ethernet sont capturés. • eth1 : Les paquets sur l'interface Ethernet 2 sont capturés. • radio0 : Les paquets passant par la radio 2,4 GHz sont capturés. • radio1 : Les paquets passant par la radio 5 GHz sont capturés. • radio2 : Les paquets passant par la radio 6 GHz sont capturés.
Taille max. Du fichier de capture (64-12288 Ko)	Entrez la taille maximale à laquelle le fichier contenant les paquets capturés est limité. La plage est de 64 à 12288 kb. La valeur par défaut est 1024 Ko. **REMARQUE:** Lorsque plusieurs interfaces sont sélectionnées, la taille totale du fichier de capture de toutes les interfaces sélectionnées doit être comprise entre 64 et 12288 Ko.
Durée de capture (10-3600 s)	Entrez la durée maximale du processus de capture (c'est-à-dire, si vous ne cliquez pas sur le bouton **arrêter**). La plage est de 10 à 3600 secondes. Par défaut, la durée maximale est de 300 secondes.

(A continué)

Paramètre	Description
Filtrer	Spécifiez une expression de filtre tcpdump pour capturer uniquement le trafic réseau souhaité. Par défaut, le filtre est défini sur **AUCUN**.
Capture promiscuous (interfaces Ethernet uniquement)	Pour permettre au système de APcapturer des paquets en mode promiscuité, cochez la case **Activer**. Par défaut, le mode promiscuité est désactivé. En mode promiscuité, la ou les radios reçoivent tout le trafic sur le canal, y compris le trafic qui n'est pas destiné au AP. En mode Capture promiscuous, l'interface Ethernet capture tout le trafic réseau sur le segment, même les paquets non adressés au AP. En mode Promiscuous Capture, l'interface continue de fonctionner normalement. Les paquets qui ne sont pas destinés au APne sont pas transférés. Lorsque le processus de capture s'arrête, l'interface repasse en mode non promiscuous.
Canal (interfaces radio uniquement)	Dans le menu canal, sélectionnez un canal spécifique pour capturer les paquets. Les clients sans fil se déconnectent et se reconnectent si vous changez de canal.

6. Pour démarrer le processus de capture de paquets, cliquez sur le bouton **Démarrer**.

   Si des paquets capturés sont déjà stockés sur le AP, vous êtes invité à autoriser le processus de capture de paquets à écraser les anciennes informations.

7. Pour arrêter le processus de capture de paquets, cliquez sur le bouton **arrêter**.

   Si vous n'arrêtez pas le processus manuellement, le processus s'arrête automatiquement lorsque la durée de capture est dépassée.

8. Pour télécharger le fichier avec les paquets capturés, procédez comme suit :
   a. Cliquez sur le bouton **Téléchargements**.
   b. Suivez les instructions de votre navigateur pour enregistrer le fichier sur votre ordinateur.

9. Pour afficher les informations les plus récentes sur la page, cliquez sur le bouton **Actualiser**.

Effectuez un test ping

Vous pouvez envoyer une requête ping à l'adresse IP d'un périphérique ou d'un emplacement réseau à partir de APet afficher les résultats du test ping.

Pour effectuer un test ping :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.
3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

     REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.
   - Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
   - NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

   Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

   Le tableau de bord s’affiche.
4. Sélectionnez **gestion > Diagnostics > test Ping** .

   La page test Ping s'affiche.
5. Spécifiez les paramètres comme décrit dans le tableau suivant.

Paramètre	Description
Nombre de ping	Nombre de pings que doit envoyer leAP. "Le nombre doit être compris entre 1 et 1024." Le numéro par défaut est 16.
Taille du paquet (en octets)	La taille de chaque paquet ping. La taille peut être comprise entre 4 et 1024 octets. La taille par défaut est de 64 octets.

(A continué)

Paramètre	Description
Intervalle ping (en secondes)	Intervalle entre les pings. L'intervalle DPD peut être compris entre 0,5 et 10 secondes. L'intervalle par défaut est de 1 seconde.
Délai ping (en secondes)	Période après laquelle un ping expire. La durée de vie de la SA peut être comprise entre 1 et 300 secondes. La période par défaut est de 60 secondes.
Hôte distant	Adresse IP à laquelle le système AP doit envoyer une requête ping. Ce champ peut contenir jusqu'à 100 caractères. L'adresse par défaut est : 8.8.8.8.

6. Pour lancer le test ping, cliquez sur le bouton **Démarrer**.

   Les résultats du test Ping s'affichent dans le champ résultat Ping.

7. Pour arrêter le test ping avant que le nombre de ping soit atteint ou si le ping expire, cliquez sur le bouton **arrêter**.

Effectuez un test de débit

Vous pouvez exécuter des tests de vitesse Internet pour vérifier la vitesse entre votre fournisseur d'accès Internet (FAI) et AP.

Pour effectuer un test de vitesse :

1. Lancez un navigateur Web à partir d'un ordinateur connecté au même réseau que le AP ou directement au APvia un câble Ethernet ou une connexion WiFi.
2. Dans la barre d'adresse du navigateur, saisissez l'adresse IP attribuée au AP.

   La page de connexion s'affiche.

   Si votre navigateur affiche un avertissement de sécurité, vous pouvez continuer ou ajouter une exception pour l'avertissement de sécurité. Pour plus d'informations, consultez la section Que faire si vous recevez un avertissement de sécurité du navigateur à la page 56.

3. Saisissez **admin** comme APnom d'utilisateur (sensible à la casse), saisissez l'un des mots de passe suivants (également sensible à la casse) associés aux APméthodes de gestion du système, puis cliquez sur le bouton **connexion**.

   Vous gérez le AP via :

   - **Interface de l’appareil** : Le mot de passe est celui que vous avez spécifié.

REMARQUE: Si vous utilisiez pour gérer via le portail cloud Netgear insight ou l'application Insight et que vous APaviez ajouté APà un emplacement réseau Insight, gérez maintenant APvia l'interface utilisateur du terminal, mais n'avez pas encore modifié le mot de passe, saisissez le mot de passe du dernier emplacement réseau Insight.

- Activer le contrôleur Le mot de passe est le mot de passe du site engage. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car le contrôleur d'engagement gère AP.
- NETGEAR Insight Le mot de passe est le mot de passe de l'emplacement réseau Insight. Cependant, la plupart des fonctions de l'interface utilisateur du périphérique sont masquées car Insight gère AP.

Pour plus d'informations sur les paramètres, reportez-vous à la section Informations d'identification de l'interface utilisateur du périphérique à la page 53.

Le tableau de bord s’affiche.

4. Sélectionnez **gestion > Diagnostics > test de vitesse** .

   La page vérification de la vitesse Internet s'affiche.

5. Pour lancer le test de vitesse, cliquez sur le bouton **test Speed**.

   Les résultats du test de vitesse s'affichent.

6. Pour arrêter le test de vitesse avant la fin du test, cliquez sur le bouton **Annuler le test**.

7. Pour afficher les résultats des tests de vitesse précédents, cliquez sur le bouton **Afficher l'historique**.

   Un tableau s'affiche avec les résultats du test de vitesse précédent.

Conseils rapides pour le dépannage WiFi

Problèmes avec un réseau WiFi

Si un ou plusieurs réseaux WiFi ne fonctionnent pas normalement, pensez à remettre sous tension le AP:

1. Débranchez le câble Ethernet du APau commutateur réseau.
2. Si vous utilisez un adaptateur secteur, déconnectez-le du AP.

3. Branchez le câble Ethernet du APau commutateur réseau. Attendez deux minutes.
4. Si vous utilisez un adaptateur secteur, connectez-le au AP. Attendez deux minutes.

Problèmes avec un client WiFi

Si un client WiFi ne parvient pas à se connecter au AP, vérifiez les points suivants :

- Assurez-vous que les radios WiFi ne sont pas désactivées. Pour plus d'informations sur les radios WiFi, reportez-vous à la section Permet d'allumer ou d'éteindre une radio à la page 113.
- Assurez-vous que les paramètres WiFi du client WiFi et AP correspondent exactement.

  Le nom du réseau WiFi (SSID) et les paramètres de sécurité WiFi du routeur et de l'ordinateur WiFi doivent correspondre exactement.

  Pour plus d'informations sur l'accès au AP pour la configuration initiale via une connexion WiFi, reportez-vous à la section Connectez-vous au AP pour la configuration initiale à la page 29.
- Assurez-vous que le client WiFi prend en charge l'authentification et le cryptage que vous utilisez pour le réseau WiFi. Pour plus d'informations, consultez la section Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90.

  REMARQUE: Si APl'authentification et le cryptage WiFi de l' sont définis sur WPA3 personnel et que le client WiFi prend en charge WPA3, assurez-vous que le pilote de périphérique de la carte WiFi est mis à jour vers la dernière version sur le client WiFi.
- Assurez-vous que le client WiFi n'est pas trop éloigné ou trop proche duAP. Pour voir si l'intensité du signal s'améliore, déplacez le client WiFi à proximité du AP mais à au moins 1,8 mètres.
- Assurez-vous que le signal WiFi n'est pas bloqué par des objets entre le AP et le client WiFi.
- Assurez-vous que APla diffusion SSID de l' n'est pas désactivée.

  Si APla diffusion SSID du est désactivée, le nom du réseau WiFi est masqué et ne s'affiche pas dans la liste de balayage du client WiFi. Pour se connecter à un réseau masqué, l'utilisateur doit saisir le nom du réseau et le mot de passe WiFi. Pour plus d'informations sur la diffusion SSID, reportez-vous à la section Masquer ou diffuser le SSID d'un réseau WiFi à la page 87.
- Assurez-vous que le client WiFi n'utilise pas d'adresse IP statique mais qu'il est configuré pour recevoir automatiquement une adresse IP avec DHCP. (Pour la plupart des périphériques, DHCP est le paramètre par défaut.)

Dépanner avec les voyants

Pour en savoir plus sur les voyants, reportez-vous à la section Voyants du panneau supérieur à la page 18.

Lorsque vous connectez le AP à une source d'alimentation et que vous n'avez pas désactivé le voyant (voir Gérer la LED à la page 279), le voyant s'allume comme décrit ici :

1. Le voyant s'allume d'abord en orange fixe, puis clignote lentement en orange. Au bout de deux minutes environ, le voyant devient vert ou bleu fixe, indiquant que la procédure de démarrage est terminée et que le AP est prêt :
   - **Vert continu** : Le point d'accès a démarré et fonctionne comme point d'accès autonome ou comme point d'accès détecté par Insight non connecté à la plateforme d'administration cloud Insight.
   - **Bleu continu** : Le PA fonctionne en mode Insight et est connecté à la plateforme d'administration cloud Insight.
2. Lorsque la procédure de démarrage est terminée, si les clients sont connectés à une radio, le voyant clignote en bleu.

Vous pouvez utiliser le voyant pour le dépannage. Pour plus d'informations, consultez la section suivante.

- Le voyant reste éteint
- Le voyant reste orange fixe
- Le AP fonctionne comme un PoE PD et le voyant clignote en vert en continu
- Le voyant clignote en orange lentement et en continu
- Le voyant ne s'allume pas en bleu en mode de gestion Netgear insight
- Le voyant ne cesse pas de clignoter en orange, vert et bleu

Le voyant reste éteint

Si vous utilisez une connexion PoE++ et que le voyant est éteint lorsque le câble Ethernet est connecté à un commutateur PoE++, procédez comme suit :

- Assurez-vous que le voyant n'est pas désactivé (voir Gérer la LED à la page 279).
- Assurez-vous que le câble Ethernet entre le AP et le commutateur PoE++ est correctement connecté aux deux extrémités.

- Assurez-vous que l'autre extrémité du câble Ethernet est branchée sur un port PoE++ d'un commutateur PoE++ alimenté.
- Assurez-vous que le bilan de puissance PoE du commutateur PoE+ n'est pas sursouscrit afin que le commutateur PoE+ puisse fournir une alimentation PoE+ (802.3at) au AP.

Si vous utilisez un adaptateur secteur en option et que le voyant reste éteint lorsque le AP est sous tension, procédez comme suit :

- Assurez-vous que le voyant n'est pas désactivé (voir Gérer la LED à la page 279).
- Assurez-vous que l'adaptateur secteur est correctement connecté à l' APet qu'il est correctement connecté à une prise secteur en état de fonctionnement. Si le cordon est branché sur une rallonge électrique, assurez-vous que cette dernière est sous tension. S'il est branché directement sur la prise murale, vérifiez que la prise n'est pas coupée.
- Assurez-vous que vous utilisez l'adaptateur secteur NETGEAR pour ce produit. Autrement dit, n'utilisez pas l'adaptateur secteur NETGEAR pour un autre produit NETGEAR ou un adaptateur secteur tiers.

Si l'erreur persiste, il est possible qu'un problème matériel existe. Pour obtenir des instructions de récupération ou de l'aide en cas de problème matériel, contactez le support technique à l'adresse netgear.com/support.

Le voyant reste orange fixe

Lorsque vous connectez le AP à une source d'alimentation, le voyant s'allume en orange fixe d'abord, puis clignote lentement en orange, puis s'allume en vert ou bleu fixe, indiquant que la procédure de démarrage est terminée et que le AP est prêt.

Si le voyant reste orange après cinq minutes, une erreur de démarrage s'est produite ou le APfonctionne mal.

Effectuez les actions suivantes :

1. Débranchez le AP de sa source d'alimentation, rebranchez-le et attendez quelques minutes pour voir si la procédure de démarrage s'est déroulée correctement.
2. Si la procédure de démarrage ne se termine toujours pas correctement et que le voyant reste orange fixe au bout de cinq minutes, utilisez le bouton **Réinitialiser** pour rétablir les paramètres par défaut duAP.

   Pour plus d'informations, consultez la section Utilisez le bouton DE RÉINITIALISATION pour réinitialiser le commutateur AP à la page 270.

Si le AP fonctionne comme un PoE PD, reportez-vous à la section Le AP fonctionne comme un PoE PD et le voyant clignote en vert en continu à la page 371.

Si l'erreur persiste, il est possible qu'un problème matériel existe. Pour obtenir des instructions de récupération ou de l'aide en cas de problème matériel, contactez le support technique à l'adresse netgear.com/support.

Le AP fonctionne comme un PoE PD et le voyant clignote en vert en continu

Lorsque vous connectez le AP à une source d'alimentation, le voyant s'allume en orange fixe d'abord, puis clignote lentement en orange, puis s'allume en vert ou bleu fixe, indiquant que la procédure de démarrage est terminée et que le AP est prêt.

Si le AP fonctionne comme un périphérique alimenté par PoE (PD) et que le voyant clignote en vert de manière continue, il est possible que le APne soit pas alimenté au niveau 802.3at (PoE+) requis. Par exemple, cette situation peut se produire si le AP est connecté à un commutateur qui fournit uniquement 802.3af (PoE) au lieu de 802.3at (PoE+).

REMARQUE: Si le AP reçoit une puissance insuffisante au niveau 802.3af (PoE), le AP réduit la puissance de transmission sur les radios 2,4 GHz et 5 GHz et désactive la radio 6 GHz.

Effectuez les actions suivantes :

1. Déconnectez et reconnectez le câble Ethernet au port LAN/PoE+ du APet au port 802.3at (PoE+) du commutateur PoE+.

   Le AP redémarre.
2. Si le voyant clignote en vert en continu, vérifiez pourquoi le commutateur PoE+ ne peut pas fournir une alimentation PoE suffisante au AP.

   Très probablement, le bilan de puissance PoE du commutateur PoE+ est sursouscrit et vous devrez peut-être déconnecter un autre terminal PoE du commutateur PoE+ pour mettre suffisamment d'énergie PoE à disposition pour le AP.

Le voyant clignote en orange lentement et en continu

Lorsque vous connectez le AP à une source d'alimentation, le voyant s'allume temporairement en orange fixe, puis devient vert ou bleu fixe, indiquant que la procédure de démarrage est terminée et que le AP est prêt. Pendant le fonctionnement normal, le voyant clignote temporairement en orange uniquement lorsque le micrologiciel est

en cours de mise à niveau. De plus, dans ce cas, le voyant clignote en orange rapidement, pas lentement.

Si le clignote en orange lentement et continuellement, le APn'a pas reçu d'adresse IP d'un serveur DHCP ou la passerelle réseau ou Internet n'est pas accessible.

Vérifiez que le client DHCP du APest activé (voir Activez le client DHCP à la page 222), que votre réseau comprend un serveur DHCP (ou un routeur fonctionnant comme un serveur DHCP) et que le serveur DHCP peut atteindre le AP (les deux doivent être sur le même réseau).

Dans le cas improbable où votre réseau n'inclut pas de serveur DHCP, vous devrez peut-être configurer une adresse IP fixe (statique) sur le AP (voir Désactivez le client DHCP et définissez une adresse IP fixe à la page 221).

Si vous utilisez une adresse IP correcte, le réseau ou la passerelle Internet n'est pas accessible. Vérifiez que les paramètres réseau ou la passerelle Internet fonctionnent correctement.

Le voyant ne s'allume pas en bleu en mode de gestion Netgear insight

Si le AP fonctionne en mode de gestion de navigateur Web, le voyant s'allume en vert. Il s'agit d'un comportement normal du voyant.

Toutefois, si le AP fonctionne en mode de gestion Netgear insight et que le voyant ne s'allume pas en bleu mais reste vert, le APn'est pas connecté à la plate-forme de gestion basée sur le cloud Insight.

Si le AP fonctionne en mode de gestion Netgear insight et que le voyant ne s'allume pas en bleu, essayez les étapes de dépannage suivantes jusqu'à ce que le problème soit résolu :

1. Vérifiez que le mode de gestion du AP est Netgear insight.

   Pour plus d'informations, consultez la section Changez le mode de gestion en Netgear insight ou navigateur Web à la page 242.
2. Assurez-vous que la connexion par câble Ethernet entre le AP et votre réseau est bonne.
3. Assurez-vous que le AP est connecté à Internet et que la connexion Internet est bonne.
4. Assurez-vous que le switch exécute la dernière version de son firmware.

   Pour plus d'informations, consultez la section Gérer le micrologiciel du AP à la page 253.

5. Déconnectez et reconnectez le câble Ethernet au port LAN/PoE++ et attendez cinq minutes pour voir si le voyant s'allume en bleu.

   Si vous utilisez un adaptateur secteur avec le AP, déconnectez et reconnectez l'adaptateur secteur et attendez cinq minutes pour voir si le voyant s'allume en bleu fixe.

6. Si le problème n'est toujours pas résolu, utilisez le bouton **Réinitialiser** pour rétablir les paramètres par défaut du APet reconfigurer le AP.

   Pour plus d'informations, consultez la section Utilisez le bouton DE RÉINITIALISATION pour réinitialiser le commutateur AP à la page 270.

Si l'erreur persiste, il est possible qu'un problème matériel existe. Pour obtenir des instructions de récupération ou de l'aide en cas de problème matériel, contactez le support technique à l'adresse netgear.com/support.

Le voyant ne cesse pas de clignoter en orange, vert et bleu

Au cours du processus d'installation et de configuration initial dans un réseau WiFi à maillage instantané Insight, le voyant clignote en orange, vert et bleu pendant la configuration du APen tant que nœud. Pour plus d'informations, consultez la section Connectez APen tant que nœud à une racine à l'aide de l'application Insight à la page 67.

Si le voyant ne cesse pas de clignoter en orange, vert et bleu, le nœud ne peut pas se connecter.

Vérifiez les éléments suivants ou essayez les étapes de dépannage suivantes :

- Assurez-vous qu'au moins une racine est disponible pour la connexion du nœud.
- Assurez-vous que toutes les racines exécutent la dernière version du micrologiciel.
- Assurez-vous que la puissance de sortie de chaque radio sur chaque racine est à son niveau maximal. Par défaut, la puissance de sortie d'une radio est à son niveau maximal. Pour plus d'informations, consultez la section Modifier la puissance de sortie d'une radio à la page 121.
- Assurez-vous que le nœud n'est pas trop éloigné d'une racine. Pour plus d'informations, consultez la section Le nœud et la racine ne peuvent pas se connecter à la page 374.
- Redémarrez le nœud.
- Supprimez le nœud de votre emplacement réseau Insight et de votre compte Insight. Ensuite, ajoutez à nouveau le nœud à votre compte Insight et à votre emplacement réseau Insight.

Le nœud et la racine ne peuvent pas se connecter

Lorsque vous ajoutez APen tant que nœud à un emplacement réseau Insight qui inclut une ou plusieurs racines (voir Connectez APen tant que nœud à une racine à l'aide de l'application Insight à la page 67), nous vous recommandons de placer le nœud dans la même pièce qu'une racine lors de la synchronisation initiale. Après une synchronisation réussie, déplacez le nœud à l'emplacement où vous souhaitez l'utiliser.

Pour une connexion WiFi fiable, placez le nœud à moins de 7,5 m (25 pieds), dans une ligne de mire, avec un minimum d'obstacles par rapport à la racine la plus proche.

Pour synchroniser le nœud et la racine après avoir déjà ajouté le nœud à un emplacement réseau Insight :

1. Placez le nœud dans la même pièce que la racine.

   Utilisez cet emplacement de satellite uniquement pendant le processus de synchronisation.
2. Branchez le satellite à une source d'alimentation.

   Si vous n'utilisez pas de connexion PoE++ à un commutateur PoE++, connectez un adaptateur secteur au connecteur d'alimentation CC.

   Le voyant du nœud s'allume en orange fixe.
3. Attendez que le nœud effectue la connexion initiale et le processus de configuration, que le voyant cesse de clignoter en orange, vert et bleu et qu'il s'allume en bleu fixe.

   REMARQUE: La connexion initiale et le processus de configuration peuvent prendre jusqu'à 10 minutes. Le nœud peut redémarrer pendant le processus de configuration.

   Le voyant s'allume comme suit pendant le processus de connexion et de configuration initial :

   - **Vert clignotant** : Le nœud tente de détecter une racine.
   - **Vert continu** : Le nœud établit sa première connexion avec la racine qui fournit le signal WiFi le plus puissant.
   - **Le voyant clignote lentement en orange** : Le nœud contacte le routeur réseau ou le serveur DHCP pour recevoir une adresse IP.

Si le voyant ne cesse pas de clignoter en orange, reportez-vous à la section Le voyant clignote en orange lentement et en continu à la page 371.

- **Orange, vert et bleu clignotants** : Le nœud est configuré en tant que périphérique géré dans le réseau WiFi maillé instantané Insight.

  Si le voyant ne cesse pas de clignoter en orange, vert et bleu, reportez-vous à la section Le voyant ne cesse pas de clignoter en orange, vert et bleu à la page 373.

Lorsque la configuration est terminée, le voyant s'allume comme suit :

- **Bleu continu** : La configuration est terminée et le nœud est prêt à fonctionner. Le nœud fonctionne dans le réseau WiFi maillé instantané Insight et est connecté au cloud Insight.

4. Déconnectez le nœud et déplacez-le à l'emplacement où vous souhaitez l'utiliser.
5. Au nouvel emplacement, répétez Étape 2 les étapes et Étape 3.
6. Attendez que le nœud se resynchronise avec la racine.

   Lorsque le voyant du nœud s'allume en bleu fixe, la synchronisation du nœud et de la racine a réussi.

   Si le nœud et la racine ne se sont pas synchronisés, rapprochez le nœud de la racine et réessayez. Le nœud doit se trouver dans la zone de couverture WiFi de la racine pour établir une connexion WiFi correcte ou correcte.

Dépannez la connectivité WiFi pour un client WiFi

Si un client WiFi ne parvient pas à se connecter au AP ou si la connectivité WiFi n'est pas normale, essayez d'isoler le problème :

- Assurez-vous que les paramètres WiFi du client WiFi et AP correspondent exactement.

  Le nom du réseau WiFi (SSID) et les paramètres de sécurité WiFi du routeur et de l'ordinateur WiFi doivent correspondre exactement. Assurez-vous que le client WiFi utilise la phrase de passe correcte pour le réseau WiFi.

  Pour plus d'informations sur l'accès au AP pour la configuration initiale via une connexion WiFi, reportez-vous à la section Connectez-vous au AP pour la configuration initiale à la page 29.
- Le client WiFi prend-il en charge l'authentification et le cryptage que vous avez configurés pour le réseau WiFi ?

  Pour plus d'informations, consultez la section Modifier l'authentification et la sécurité d'un réseau WiFi à la page 90.

REMARQUE: Si APl'authentification et le cryptage WiFi de l' sont définis sur WPA3 personnel et que le client WiFi prend en charge WPA3, assurez-vous que le pilote de périphérique de la carte WiFi est mis à jour vers la dernière version sur le client WiFi.

- Assurez-vous que les radios WiFi ne sont pas désactivées. Pour plus d'informations sur les radios WiFi, reportez-vous à la section Permet d'allumer ou d'éteindre une radio à la page 113.
- Si vous avez désactivé APla diffusion SSID du pour le réseau WiFi, le réseau WiFi est masqué et ne s'affiche pas dans la liste d'analyse du réseau du périphérique WiFi. (Par défaut, la diffusion SSID est activée.) Pour plus d'informations sur la diffusion SSID, reportez-vous à la section Masquer ou diffuser le SSID d'un réseau WiFi à la page 87.

REMARQUE: Si vous souhaitez modifier les paramètres d'un réseau WiFi sur le AP, utilisez une connexion LAN filaire pour éviter d'être déconnecté lorsque les nouveaux paramètres WiFi prennent effet.

Si le client WiFi détecte le réseau WiFi mais que la puissance du signal est faible, vérifiez les conditions suivantes :

- Le client WiFi est-il trop éloigné du AP, ou trop proche ?

  Placez votre ordinateur près du routeur, à une distance d'au moins 6 mètres (1.8 pieds), et vérifiez si la puissance du signal s'améliore.
- Des objets entre le client WiFi et le bloquent-ils le APsignal WiFi ?

Dépannage de la navigation Internet

Si un périphérique WiFi est connecté à APmais ne parvient pas à charger de pages Web à partir d'Internet, cela peut être dû à l'une des raisons suivantes :

- Il est possible que le périphérique WiFi ne reconnaisse aucune adresse de serveur DNS.

  Si vous avez saisi manuellement une adresse DNS lors de la configuration de AP (c'est-à-dire que APutilise les paramètres d'adresse IP statique), redémarrez le périphérique WiFi et vérifiez l'adresse DNS.
- Il est possible que le périphérique WiFi n'utilise pas les paramètres TCP/IP corrects.

  Si le périphérique WiFi obtient ses informations via DHCP, redémarrez-le et vérifiez l'adresse du commutateur ou du modem Internet auquel est connecté leAP.

Pour plus d'informations sur les problèmes TCP/IP, reportez-vous à la section Dépannez votre réseau à l'aide de l'utilitaire ping à la page 379.

Vous ne pouvez pas vous connecter à APvia une connexion LAN

Si vous ne parvenez pas à vous connecter à à APà partir d'un ordinateur de votre réseau local et à utiliser APl'interface utilisateur du périphérique de, vérifiez les points suivants :

- Assurez-vous d'utiliser les informations de connexion correctes. Le nom d'utilisateur est **admin** et le mot de passe est celui que vous avez spécifié. Le nom utilisateur et le mot de passe sont sensibles à la casse.

  Si vous avez précédemment ajouté APà un emplacement réseau Netgear insight et géré APvia le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour cet emplacement. Pour plus d'informations, consultez la section Connectez-vous via WiFi à l'aide de l'application Netgear insight à la page 34.
- Assurez-vous que l'adresse IP de votre ordinateur se trouve sur le même sous-réseau que le routeur.

  Si vous avez désactivé le APclient DHCP du et configuré une adresse IP fixe (statique) lorsque vous avez connecté le AP à votre réseau (voir Désactivez le client DHCP et définissez une adresse IP fixe à la page 221), définissez l'adresse IP et le masque de sous-réseau de votre ordinateur sur de sorte que les adresses IP de votre ordinateur et du AP se trouvent dans le même sous-réseau IP.
- Quittez le navigateur et relancez-le.
- Si vous utilisez sur un ancien type de navigateur, assurez-vous que Java, JavaScript ou ActiveX est activé dans votre navigateur. Si vous utilisez Internet Explorer, cliquez sur **le** bouton Actualiser pour vous assurer que l'applet Java est chargée.
- Si APl'adresse IP de votre a été modifiée (par exemple, le serveur DHCP de votre réseau a émis une adresse IP au AP) et que vous ne connaissez pas l'adresse IP actuelle, utilisez une application de scanner IP pour détecter l'adresse IP.

  REMARQUE: Vous pouvez également utiliser l'application Netgear insight pour découvrir l'adresse IP attribuée au AP. Pour plus d'informations, consultez la section Connectez-vous via WiFi à l'aide de l'application Netgear insight à la page 34.

  Si vous ne trouvez toujours pas l'adresse IP, réinitialisez APla configuration par défaut de l' sur les paramètres d'usine. Ceci définit APl'adresse IP du sur 192.168.0.100 et

active le client DHCP. Pour plus d'informations, consultez la section Utilisez le bouton DE RÉINITIALISATION pour réinitialiser le commutateur AP à la page 270.

Les modifications ne sont pas enregistrées

Si vous êtes connecté à l'APinterface utilisateur du terminal de et que APn'enregistre pas les modifications apportées à une page, procédez comme suit :

- Lorsque vous entrez les paramètres de configuration, cliquez toujours sur **le** bouton appliquer avant de passer à une autre page ou un autre onglet, sinon vos modifications sont perdues.
- Cliquez sur le bouton **Actualiser** ou **Rafraîchir** du navigateur Web. Il est possible que les modifications se soient produites mais que les anciens paramètres restent dans le cache du navigateur Web.

Vous entrez un mot de passe incorrect et ne pouvez plus vous connecter à AP

Si vous entrez un mot de passe administrateur erroné cinq fois, l'accès à l'APinterface utilisateur du terminal de l' est bloqué pendant cinq minutes.

Au bout de cinq minutes, le compteur de tentatives de connexion infructueuses est réinitialisé et vous pouvez tenter de vous reconnecter.

En outre, les règles suivantes s'appliquent au nombre d'échecs de tentatives de connexion :

- La dernière tentative d'accès détermine si le compteur de tentatives de connexion échouées est augmenté.
- Si vous redémarrez AP, le compteur des tentatives de connexion échouées est réinitialisé.

Dépannez votre réseau à l'aide de l'utilitaire ping

La plupart des périphériques et routeurs réseau contiennent un utilitaire ping qui envoie un paquet de demande d’écho au périphérique désigné. Le périphérique répond ensuite avec une réponse d'écho. Vous pouvez facilement dépanner un réseau à l'aide de l'utilitaire ping de votre ordinateur ou de votre station de travail.

Testez le chemin LAN vers votre routeur AP

Vous pouvez envoyer une requête ping au routeur à partir de votre ordinateur pour vérifier que le chemin du réseau local vers votre routeur est correctement configuré.

Pour envoyer une requête ping au routeur à partir d'un ordinateur Windows :

1. Depuis la barre d'outils Windows, cliquez sur le bouton **Démarrer**, puis sélectionnez **Exécuter**.
2. Dans le champ prévu à cet effet, tapez **ping** suivi de l'adresse IP du routeur, comme dans cet exemple :

   ping 192.168.0.100
3. Cliquez sur le bouton **OK**.

   Un message tel que le suivant s'affiche :

   ```
   Pinging <IP address> with 32 bytes of data
   ```

   Si la connexion est établie, le message suivant apparaît :

   ```
   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
   ```

   Si la connexion échoue, le message suivant apparaît :

   ```
   Request timed out
   ```

Si le chemin ne fonctionne pas correctement, l'un des problèmes suivants peut se produire :

- Mauvaises connexions physiques.

  Vérifiez que les voyants appropriés sont allumés pour vos périphériques réseau. Si votre routeur et votre ordinateur sont connectés à un commutateur Ethernet distinct, assurez-vous que les voyants de liaison sont allumés pour les ports de commutateur connectés à votre ordinateur et à votre routeur.
- Mauvaise configuration réseau.

Vérifiez que l'adresse IP de votre routeur et de votre ordinateur est correcte et que les adresses se trouvent sur le même sous-réseau.

Tester le chemin de votre ordinateur vers un périphérique distant

Après avoir constaté que le chemin du réseau local fonctionne correctement, testez le chemin de votre ordinateur vers un périphérique distant.

Testez le chemin de votre ordinateur vers un périphérique distant :

1. Depuis la barre d'outils Windows, cliquez sur le bouton **Démarrer**, puis sélectionnez **Exécuter**.
2. Dans le champ prévu à cet effet, entrez **ping -n 10** *adresse IP* .

   Où *<IP address>* est l'adresse IP d'un périphérique distant tel que votre serveur DNS ISP.

Si le chemin fonctionne correctement, répond comme décrit à la section Testez le chemin LAN vers votre routeur AP à la page 379 affichage. Si vous n'obtenez aucun message, procédez comme suit :

- Vérifiez que votre ordinateur répertorie l'adresse IP du routeur auquel est connecté le APen tant que routeur par défaut. Si la configuration IP de votre ordinateur est attribuée par DHCP, ces informations ne sont pas visibles dans le panneau de configuration réseau de votre ordinateur.
- Vérifiez que l'adresse réseau de votre ordinateur (la partie de l'adresse IP spécifiée par le masque de réseau) est différente de l'adresse réseau du périphérique distant.

A

Paramètres usine par défaut et caractéristiques techniques

Cette annexe est composée des sections suivantes :

- Paramètres par défaut
- Caractéristiques techniques

Paramètres par défaut

Vous pouvez rétablir les paramètres par défaut duAP, indiqués dans le tableau suivant.

Pour plus d'informations sur la réinitialisation des paramètres par défaut duAP, reportez-vous à la section Rétablissez les paramètres par défaut du routeur à la page 269.

Table 4 : Paramètres par défaut

Fonction	paramètre par défaut
Paramètres de gestion et de connexion	
Modes de gestion	Netgear insight (Cloud/distant) **Remarque** : Pour accéder à l'interface utilisateur du périphérique, vous devez sélectionner navigateur Web (local) comme mode de gestion.
Adresse de connexion pour l'utilisateur	192.168.0,100, s'il n'est pas connecté à un réseau. **Remarque** : S'il est connecté à un réseau, le AP reçoit une adresse IP d'un serveur DHCP ou d'un routeur du réseau.
Nom d'utilisateur	**admin**, non configurable
Mot de passe de connexion AP	**mot de passe**, sensible à la casse, configurable **Remarque** : La première fois que vous vous connectez à l'interface utilisateur de l'appareil, vous devez modifier le mot de passe de connexion AP. Si vous avez précédemment ajouté APà un emplacement réseau Netgear insight et géré APvia le portail cloud Insight ou l'application Insight, saisissez le mot de passe réseau Insight pour cet emplacement. Pour plus d'informations, voir Connectez-vous sur Internet à l'aide du portail cloud Netgear insight à la page 32 ou Connectez-vous via WiFi à l'aide de l'application Netgear insight à la page 34.
Paramètres réseau WiFi pour la configuration initiale et la connexion WiFi	
Nom SSID initial	Le SSID de la configuration initiale est NETGEARxxxxxx-SETUP, où xxxxxx correspond aux six derniers chiffres hexadécimaux de APl'adresse MAC de l' . **Remarque** : La première fois que vous vous connectez à l'interface utilisateur du périphérique, vous devez modifier le SSID. Si vous avez précédemment ajouté APà un emplacement réseau Netgear insight et géré APvia le portail cloud Insight ou l'application Insight, cette exigence peut ne pas s'appliquer.
Sécurité WiFi initiale	WPA3/WPA2 Personal (WPA3-PSK/WPA2-PSK) Mot de passe WiFi (clé réseau) : **sharedsecret** **Remarque** : La première fois que vous vous connectez au commutateur, vous devez modifier le mot de passe par défaut. Si vous avez précédemment ajouté APà un emplacement réseau Netgear insight et géré APvia le portail cloud Insight ou l'application Insight, cette exigence peut ne pas s'appliquer.

Table 4 : Paramètres par défaut (A continué)

Fonction	paramètre par défaut
Canal radio	Automatiquement sélectionné (Auto) pour toutes les radios. **Remarque** : Les canaux disponibles et pris en charge dépendent du pays et de la région que vous sélectionnez pour le AP.
Paramètres généraux du système	
Mode de fonctionnement	Mode AP
Client DHCP	Activé pour que le AP reçoive une adresse IP d'un serveur DHCP ou d'un routeur du réseau.
Client NTP	Sous tension
Protocole STP	Désactivé(e)
Vérification de l'intégrité du réseau	Désactivé(e)
Protocole IGMP Snooping	Désactivé(e)
Chemin de données assisté par matériel	Sous tension
VLAN 802.1Q	VLAN non étiqueté avec VLAN ID 1
VLAN de gestion	Identifiant VLAN
Syslog	Désactivé(e)
LLDP Ethernet	Sous tension
UPnP	Sous tension
Voyant	Sous tension
Mode efficacité énergétique	Désactivé(e)
Passerelle DNS multicast	Désactivé(e)
Paramètres WLAN pour un réseau WiFi individuel (SSID ou VAP)	
Diffuser le SSID	Sous tension
ID VLAN (pour les clients WiFi)	1
Authentification du réseau	WPA3/WPA2 Personal (WPA3-PSK/WPA2-PSK) Le chiffrement des données non configurable pour WPA3 est SAE Le chiffrement des données non configurable pour WPA2 est AES
802.11w (PMF)	En option

Table 4 : Paramètres par défaut (A continué)

Fonction	paramètre par défaut
Multi PSK	Désactivé(e) Multi PSK est disponible uniquement lorsque l'authentification est WPA2 personnel ou WPA2/WPA personnel.
Fonctionnement multi-liaisons	Désactivé(e)
Programme de diffusion	Toujours activé
Bande radio	2,4 GHz et 5 GHz activés mais 6 GHz désactivés
Redirection de bande	Désactivé(e)
Adressage et trafic	Pont
Isolation du client WiFi	Désactivé(e)
Suivi d'URL	Désactivé(e)
ACL MAC pour l'accès client WiFi	Aucune assignation
ACL MAC pour le trafic haut débit et multicast des clients WiFi	Aucune assignation
Groupe de filtres de trafic MAC/IP	Aucune assignation
Portail captif	None (Aucun)
Liste de contrôle d'accès (ACL) MAC	Aucune assignation
Limitation du débit	None (Aucun)
Sélection avancée du tarif	Débit de multidiffusion fixe : 11 Mbit/s pour la radio 2,4 GHz et 24 Mbit/s pour la radio 5 GHz Contrôle du débit : Désactivé(e) Niveau de densité : 0
Paramètres radio de base qui s'appliquent à tous les réseaux WiFi (SSID ou VPN)	
Diffusion radio	Radio 2,4 GHz : Sous tension Radio 5 GHz : Sous tension Radio 6 GHz : Sous tension
Mode WiFi	Radio 2,4 GHz : mode 11be, qui prend également en charge 11ax, 11b, 11bg et 11na Radio 5 GHz : mode 11be, qui prend également en charge 11a, 11na, 11ac et 11ax Radio 6 GHz : mode 11be, qui prend également en charge 11ax

Table 4 : Paramètres par défaut (A continué)

Fonction	paramètre par défaut
Largeur du canal	Radio 2,4 GHz : 20 MHz Radio 5 GHz : 40 MHz Radio 6 GHz : 80 MHz
Intervalle de garde	Radio 2,4 GHz : Long-800 ns Radio 5 GHz : Long-800 ns Radio 6 GHz : Long-800 ns
Puissance de sortie	Radio 2,4 GHz : Maximum (100 %) Radio 5 GHz : Maximum (100 %) Radio 6 GHz : Maximum (100 %)
Canal	Radio 2,4 GHz : Automatique Radio 5 GHz : Automatique Radio 6 GHz : Automatique
Wi-Fi Multimedia (WMM)	Radio 2,4 GHz : Sous tension Radio 5 GHz : Sous tension Radio 6 GHz : Sous tension
Économie d'énergie WMM	Radio 2,4 GHz : Sous tension Radio 5 GHz : Sous tension Radio 6 GHz : Sous tension
Paramètres radio avancés qui s'appliquent à tous les réseaux WiFi (SSID ou VPN)	
Nombre de clients WiFi	Radio 2,4 GHz : 200 par défaut (également le nombre maximum) Radio 5 GHz : 200 par défaut (également le nombre maximum) Radio 6 GHz : 200 par défaut (également le nombre maximum)
Seuil RTS	Radio 2,4 GHz : Activé à 2346 Radio 5 GHz : Activé à 2346 Radio 6 GHz : Activé à 2346
Intervalle de balise	Radio 2,4 GHz : 100 millisec. Radio 5 GHz : 100 millisec. Radio 6 GHz : 100 millisec.
802.11n 256 QAM	Radio 2,4 GHz : Activé (s'applique uniquement en mode WiFi 11ng) Radio 5 GHz : Non configurable Radio 6 GHz : Non configurable

Table 4 : Paramètres par défaut (A continué)

Fonction	paramètre par défaut
MU-MIMO	Radio 2,4 GHz : Sous tension Radio 5 GHz : Sous tension Radio 6 GHz : Sous tension
Intervalle DTIM	Radio 2,4 GHz : 3 Radio 5 GHz : 3 Radio 6 GHz : 3
Limitation du débit de diffusion et de multidiffusion	Radio 2,4 GHz : Activé avec une limite de 64 ppps Radio 5 GHz : Activé avec une limite de 64 ppps Radio 6 GHz : Activé avec une limite de 64 ppps
Équilibrage de charge entre les radios	Désactivé(e)
Forcer les clients rémanents à se dissocier	Désactivé(e)
Proxy ARP	Sous tension
Remplacement du nom d'hôte	None (Aucun)
Pont sans fil	Aucun configuré
Sécurité	
serveurs RADIUS	Aucun configuré
Détection des points d'accès voisins	Radio 2,4 GHz : Désactivé(e) Radio 5 GHz : Désactivé(e) Radio 6 GHz : Désactivé(e)
Listes de contrôle d'accès MAC globales pour le trafic de diffusion et de multidiffusion à partir du réseau local câblé	Aucun configuré
Filtre antibruit sans fil	Huit stratégies de trafic par défaut, toutes désactivées
Filtre de trafic global	Aucune stratégie de trafic configurée
Profil application QoS	Plusieurs règles de trafic par défaut, toutes désactivées
Profil de règle globale	Aucune stratégie de trafic configurée
Listes de contrôle d'accès MAC pour l'accès client WiFi	Huit listes de contrôle d'accès par défaut, mais aucune configurée avec des adresses MAC

Table 4 : Paramètres par défaut (A continué)

Fonction	paramètre par défaut
Listes de contrôle d'accès MAC pour le trafic de diffusion et de multidiffusion des clients WiFi	Huit listes de contrôle d'accès par défaut, mais aucune configurée avec des adresses MAC
Filtres de trafic MAC/IP pour les réseaux WiFi	Huit groupes par défaut, mais aucun configuré avec des stratégies de trafic
Sécurité L2	Désactivé(e)
Protection contre les dénis de service	Désactivé(e)
Gestion à distance	
SNMP	Désactivé(e)
Autre	
Remplacement du nom d'hôte	Aucun configuré

Caractéristiques techniques

Le tableau suivant présente les caractéristiques techniques.

Table 5 : Caractéristiques techniques

Fonction	Description
Modes WiFi	Radio 2,4 GHz : 802.11be, 802.11ax, 802.11ng, 801.11bg et 802.11b. Radio 5 GHz : 802.11be, 802.11ax, 802.11ac, 802.11na et 802.11a. Radio 6 GHz : 802.11be et 802.11ax Le AP prend en charge le fonctionnement simultané dans les bandes radio 2,4 GHz, 5 GHz et 6 GHz.
Débit théorique maximal	Débit simultané d'environ 9,4 Gbit/s (688 Mbit/s dans la bande de 2,4 GHz, 2882 Mbit/s dans la bande de 5 GHz et 5765 Mbit/s dans la bande de 6 GHz). **Remarque** : Le débit peut varier. L'état du réseau et les conditions d'utilisation, notamment le volume du trafic réseau, les matériaux et la structure du bâtiment ainsi que le surdébit du réseau, réduisent la vitesse réelle de transmission des données.
Nombre maximal de clients pris en charge	Radio 2,4 GHz : 200 Radio 5 GHz : 200 Radio 6 GHz : 200

Table 5 : Caractéristiques techniques (A continué)

Fonction	Description
802.11 sécurité	WPA3 personnel, WPA3 entreprise, WPA3/WPA2 personnel, WPA2 personnel, WPA2 entreprise, WPA2/WPA personnel, Open Enhanced et Open
Standard Wifi	WiFi Multimedia Prioritization (WMM) Systèmes WDS (Wireless Distribution System)
simultanés	Radio 2,4 GHz : 2 flux (antenne 2x2) Radio 5 GHz : 2 flux (antenne 2x2) Radio 6 GHz : 2 flux (antenne 2x2)
Plage de fréquence de fonctionnement	Bande 2,4 GHz 2,412-2,462 GHz Bande 5 GHz 5,18-5,825 GHz Bande 6 GHz 5,925-7,125 GHz
Power over Ethernet	Si vous n'utilisez pas d'adaptateur secteur, le port LAN/PoE nécessite une alimentation 802.3at (PoE+). **Remarque** : PoE peut être considéré comme un environnement réseau 0 selon CEI TR 62101, et donc les circuits ITE interconnectés peuvent être considérés comme une très basse tension de sécurité (TBTS).
Consommation PoE	25 W
Adaptateur secteur	12 VCC., 2,5 A L'adaptateur secteur est localisé pour le pays de vente.
Interface matérielle	Un port Ethernet LAN/PoE RJ-45 prenant en charge 2,5 Gbit/s, 1 Gbit/s et 100 Mbit/s. Le port prend également en charge Auto Uplink (Auto MDI-X). **Remarque :** Sans adaptateur secteur, le port LAN/PoE nécessite 802.3at (PoE+).
Dimensions (L x P x H)	6,18 x 6,18 x 1,57 po (157 x 157 x 40 mm)
Poids	0,69 kg (1,52 lb)
Température de fonctionnement	0 à 40 °C (32 à 104 °F)
Humidité de fonctionnement	5 à 95 % d'humidité relative maximum, sans condensation
Température de stockage	–22° à 158°F (–30° à 70°C)
Hygrométrie de stockage	5 à 95 % d'humidité relative maximum, sans condensation
Certification EMI	Rapport FCC partie 15 (EMI) sous-partie B Rapport CEM ce, rapport en 55032/24/35 Rapport CEM en 301 489-17

Table 5 : Caractéristiques techniques (A continué)

Fonction	Description
Conformité réglementaire US	Subvention FCC FCC Spectrum Report, partie 15, sous-partie C (15.247) FCC Spectrum Report, partie 15, sous-partie E (15.407) Rapport FCC DFS Rapport sur le taux d'absorption standard (MPE) FCC
Conformité réglementaire Europe	En 300 328 rapport sur le spectre radioélectrique En 301 893 rapport sur le spectre radioélectrique En 301 893 rapport DFS Rapport en 303 687 EXPOSITION RF EN (MPE)
Sécurité et conformité énergétique	Certificat et rapport de test CEI 62368-1, ce CEI 62368-1