Dépannage des problèmes sans fil avec Catalyst Center

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Collecter des données depuis Catalyst Center

Problème avec le contrôleur sans fil Catalyst 9800

- Vérification de l'état du contrôleur avec le périphérique 360

Problème avec un point d'accès

- Captures intelligentes pour point d'accès
  - Capture de statistiques AP
  - Capture de renifleur OTA
  - Détection des anomalies

Problème de connectivité client sans fil

- Captures intelligentes pour les clients sans fil
  - Intégration de la capture de paquets
  - Capture de paquets complète

Isoler les problèmes de service réseau (AAA, DHCP, DNS)

Raisonneur de réseau

Références techniques

Introduction

Ce document décrit le dépannage des problèmes de connectivité du contrôleur LAN sans fil (WLC), du point d'accès et du client Catalyst 9800 à l'aide de Cisco Catalyst Center.

Conditions préalables

- Le contrôleur LAN sans fil doit être ajouté à Catalyst Center et afficher l'état Managed dans l'inventaire.
- L'état de télémétrie sur le WLC doit apparaître Up.

Exigences

Cisco vous recommande d'avoir connaissance des sujets suivants :

- Accès au contrôleur LAN sans fil via l'interface de ligne de commande ou l'interface utilisateur graphique
- Accès à Catalyst Center via l'interface de ligne de commande (CLI) ou l'interface utilisateur graphique (GUI)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Modèle WLC 9800
- Cisco IOS XE 17.15.5 version
- Version 2.3.7 de Catalyst Center

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

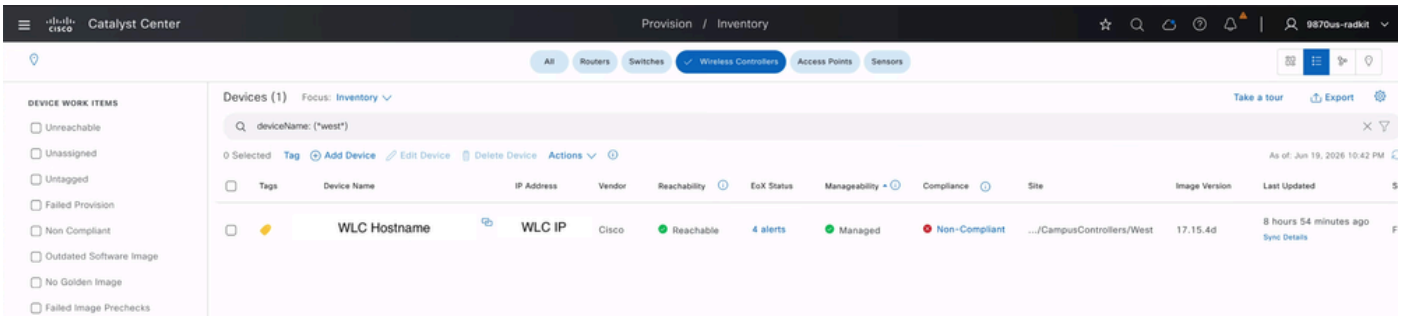
Collecter des données depuis Catalyst Center

Une fois qu'un WLC de la gamme Catalyst 9800 est ajouté à Catalyst Center for Assurance, la plate-forme extrait les données via plusieurs méthodes de collecte : interrogation SNMP, télémétrie en continu, NetFlow, Syslog, collecte basée sur l'interface de ligne de commande, API et IP SLA. Chaque mécanisme a une fonction différente : certains signalent l'état de base des périphériques (processeur, mémoire, indicateurs de performance clés), tandis que d'autres fournissent des détails précis (état PoE, sessions client, performances sans fil).

1. État des périphériques/inventaires (SNMP + CLI) : Accessibilité, CPU, mémoire, statistiques d'interface et version logicielle, collectées via l'interrogation SNMP standard et l'interface de ligne de commande.
2. Syslog: Les messages du journal système et opérationnel sont envoyés à Catalyst Center, qui agit en tant que serveur syslog configuré.
3. Télémétrie sans fil (diffusion en continu NETCONF/YANG) : Le flux Assurance de base. Il transmet les données au niveau du point d'accès et du client en temps quasi réel : événements d'intégration et d'itinérance du client, RSSI/SNR, statistiques radio/RF du point d'accès et compteurs d'intégrité internes du WLC.

Pour recevoir ces données, le contrôleur de réseau local sans fil doit être à l'état géré sur Catalyst

Center, avec l'état de télémétrie affiché entre le contrôleur 9800 et Catalyst Center.



État du contrôleur LAN sans fil sur Catalyst Center

<#root>

WLC#

show telemetry connection all

Telemetry connections

Index	Peer Address	Port	VRF	Source Address	State	State Description
0	CATC_IP	25103	0	WLC_IP	Active	Connection up

Par défaut, Cisco Catalyst Center est configuré avec des paramètres d'état, de problèmes et d'événements qui incluent des seuils et des priorités spécifiques pour les contrôleurs sans fil, les points d'accès, les clients sans fil et les applications. Catalyst Center génère des événements et des alertes en fonction des données qu'il reçoit de ces périphériques gérés et des paramètres d'événements configurés. En outre, des profils personnalisés peuvent être créés pour personnaliser ces paramètres en fonction des exigences spécifiques du réseau, ce qui permet une surveillance et des alertes plus précises en fonction des besoins uniques de l'environnement réseau.

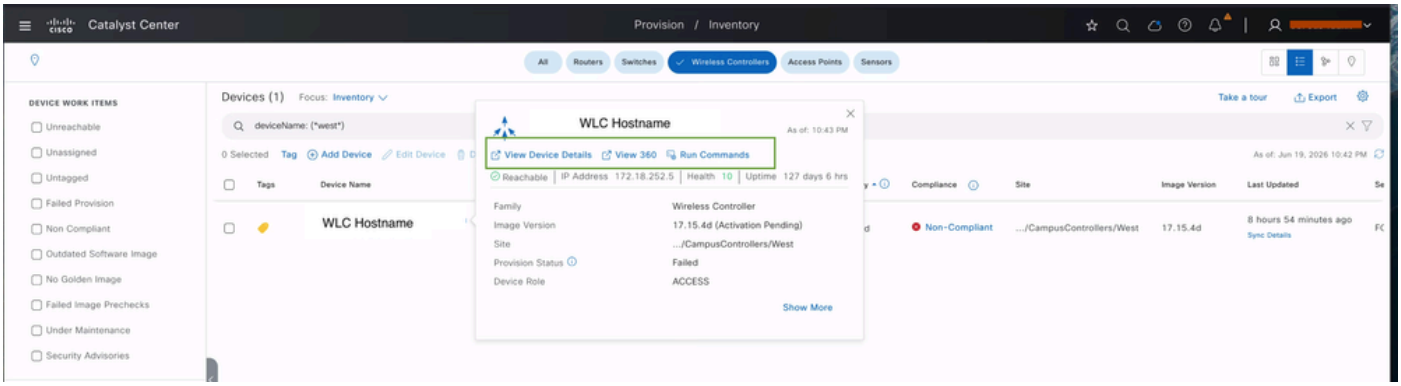
Problème avec le contrôleur sans fil Catalyst 9800

Lorsqu'un contrôleur de réseau local sans fil (WLC) rencontre des problèmes tels qu'une perte d'accessibilité, des performances lentes, des erreurs d'accessibilité, une panne ou une dégradation dans un service spécifique, Cisco Catalyst Center offre une visibilité intégrée qui vous permet de reconstruire ce qui se passait sur le contrôleur au moment exact du problème, sans avoir besoin de vous connecter directement au périphérique.

Vérification de l'état du contrôleur avec le périphérique 360

La vue Device 360 consolide l'accessibilité des contrôleurs, l'état de télémétrie, les problèmes historiques, les événements générés et les statistiques de performances dans un tableau de bord unique piloté par chronologie, ce qui en fait le premier endroit à examiner lors de l'enquête sur un problème de WLC signalé.

Accédez à Provisionner > Inventaire > Contrôleur sans fil > [recherchez le contrôleur] > cliquez sur le nom du périphérique > Périphérique 360.

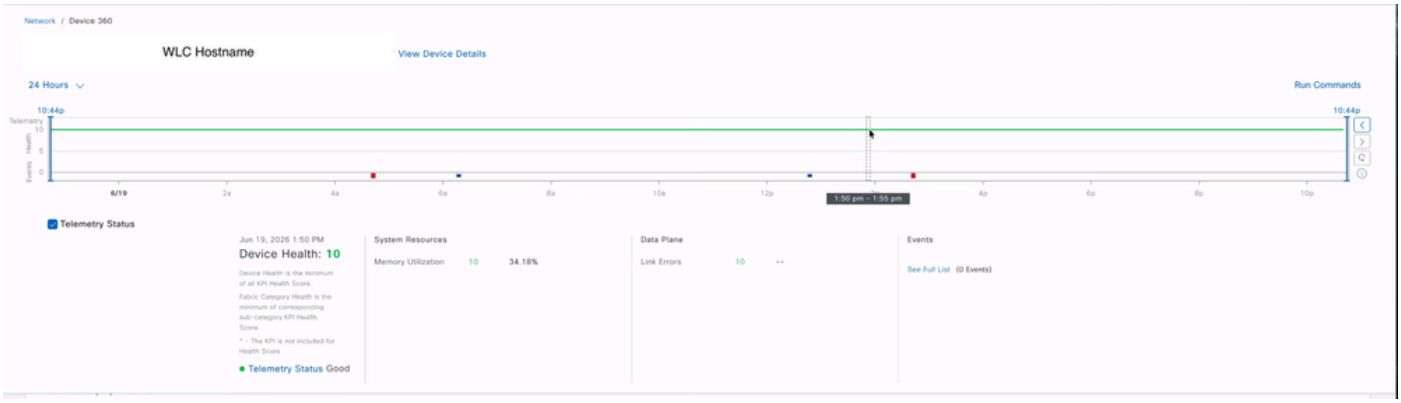


View 360 pour contrôleur LAN sans fil

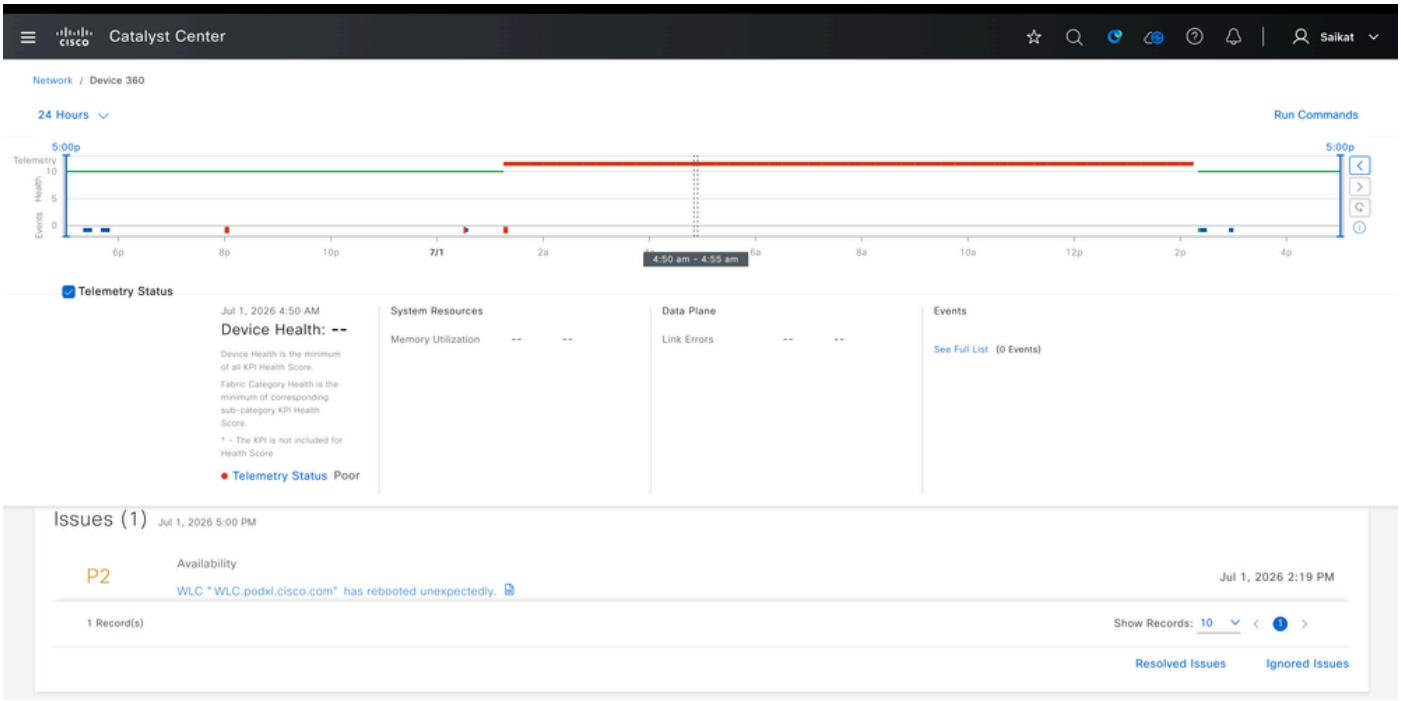
Remarque : Vous pouvez également accéder à la même vue à partir de Assurance > Health > Network, puis en cliquant sur le nom du périphérique dans le tableau Network Devices.

Le périphérique 360 vous permet de déplacer le curseur de chronologie de l'état vers n'importe quel point de la fenêtre historique prise en charge (les données Catalyst Center Assurance sont conservées pendant 30 jours maximum) pour voir exactement à quoi ressemblait l'état du contrôleur au moment de l'incident. Pour cette fenêtre sélectionnée, les surfaces de vue :

Accessibilité du périphérique : indique si le contrôleur était accessible et géré.
Telemetry status : état de l'alimentation de télémétrie SNMP/Syslog/NETCONF Assurance.

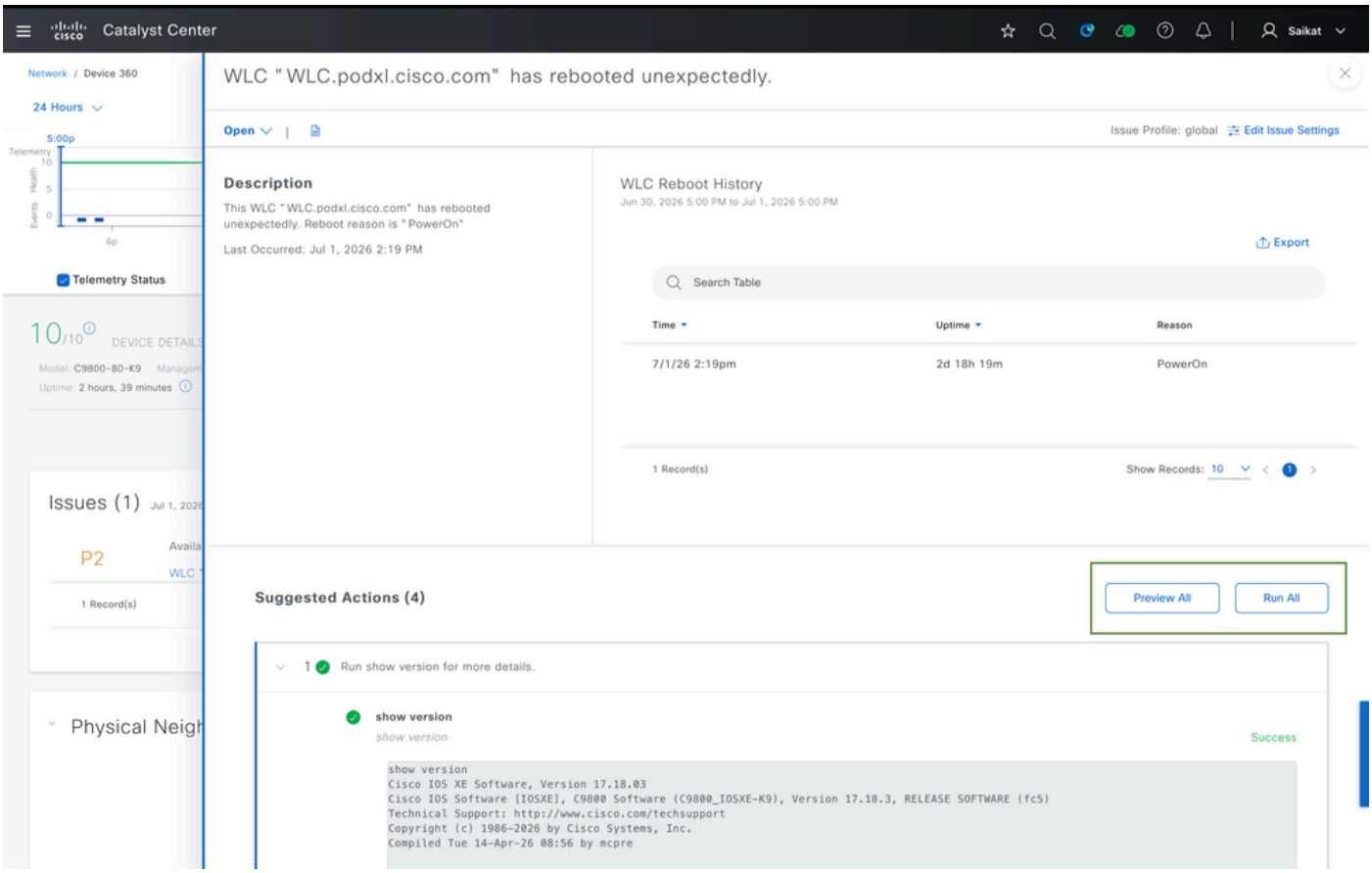


Problèmes observés — Problèmes détectés par l'assurance sur le périphérique pendant cette période.

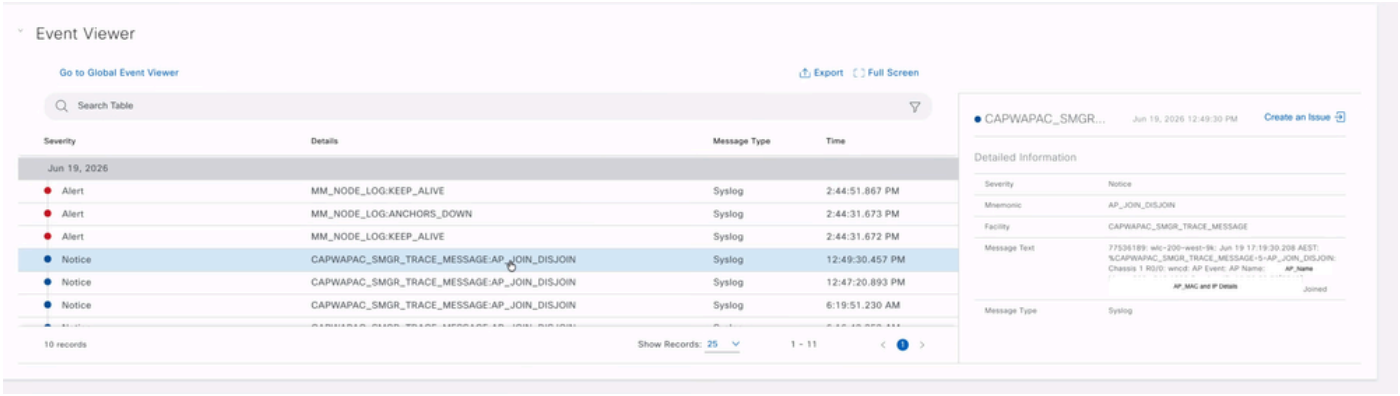


Problèmes signalés pour le contrôleur LAN sans fil

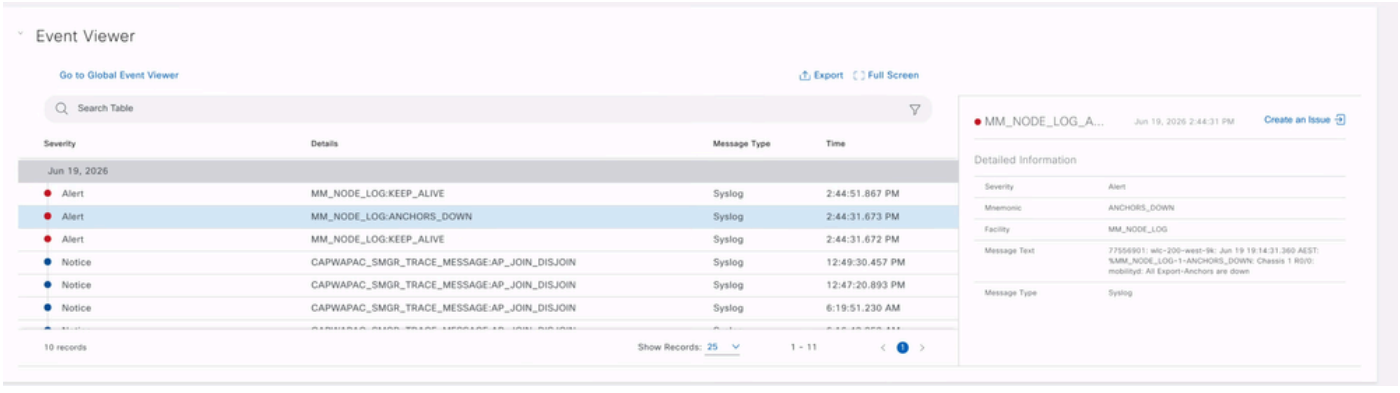
En cliquant sur un problème spécifique, vous pouvez afficher des informations détaillées le concernant, ainsi que des suggestions d'actions pour le résoudre ou approfondir l'enquête.



Action suggérée pour le problème signalé sur le WLC



Observateur d'événements pour contrôleur LAN sans fil - Exemple 1

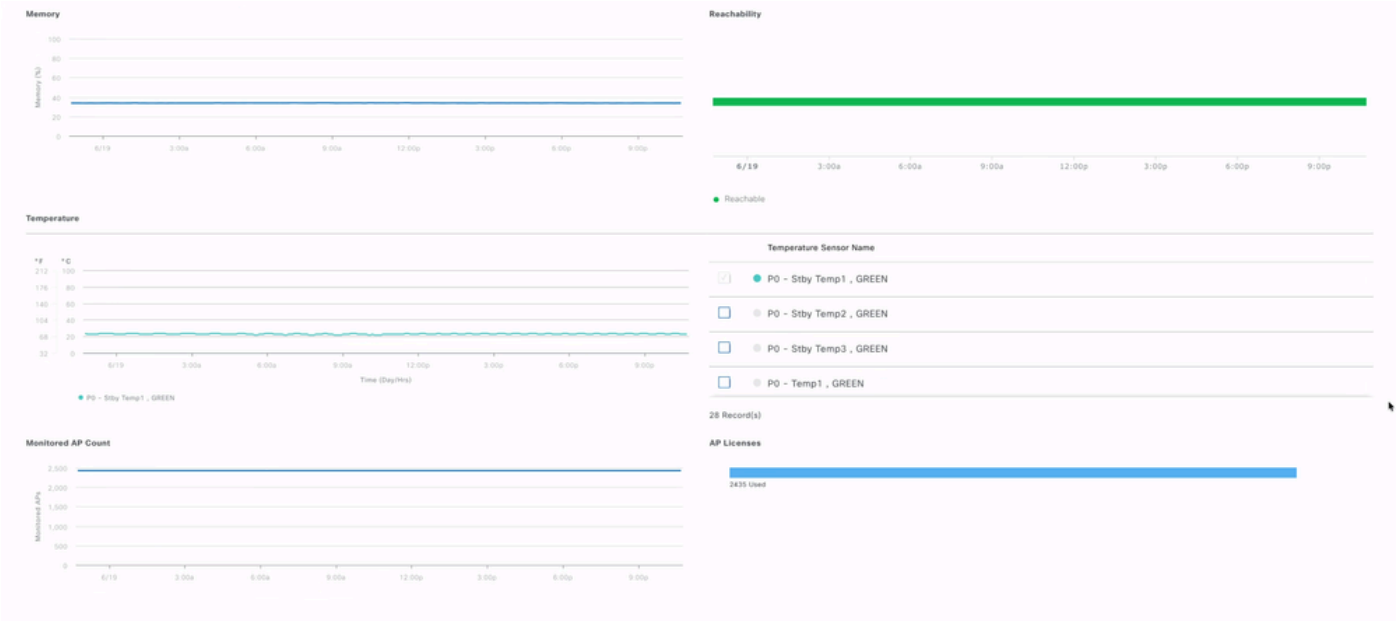


Statistiques de performances : utilisation du processeur et de la mémoire, température, temps de fonctionnement, état de haute disponibilité et raison du dernier rechargement.

Clients connectés, y compris les ventilations par nombre de clients locaux, étrangers, d'ancrage et inactifs.
AP status : état de jonction/d'intégrité des points d'accès associés au contrôleur.

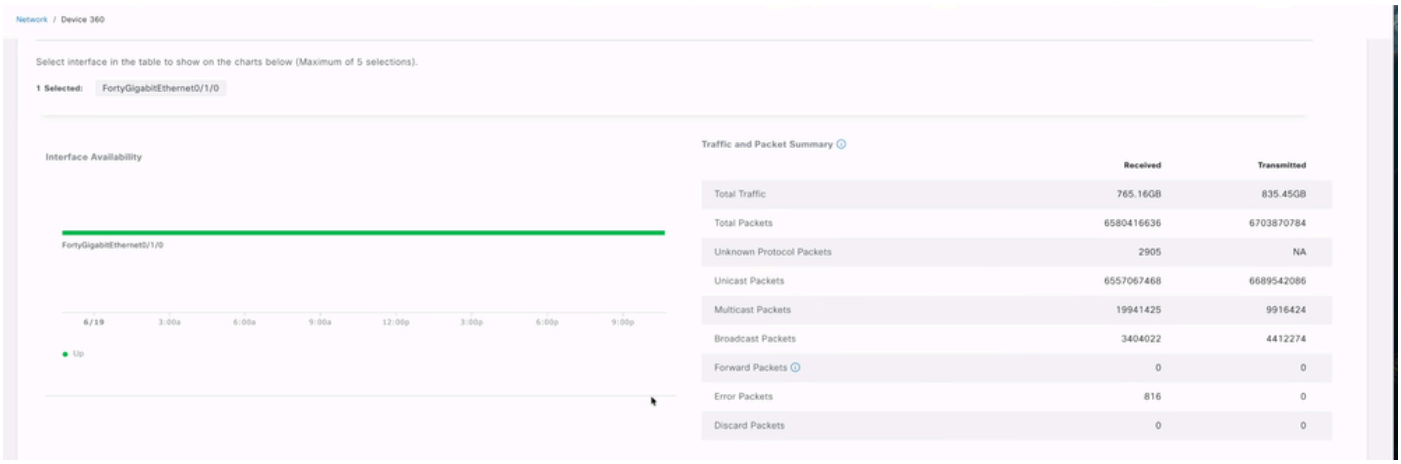


Statistiques WLC sur Catalyst Center



Statistiques WLC sur Catalyst Center

Statistiques d'interface : état par interface, nombre de paquets RX/TX, utilisation, rejets et erreurs.



Statistiques WLC sur Catalyst Center



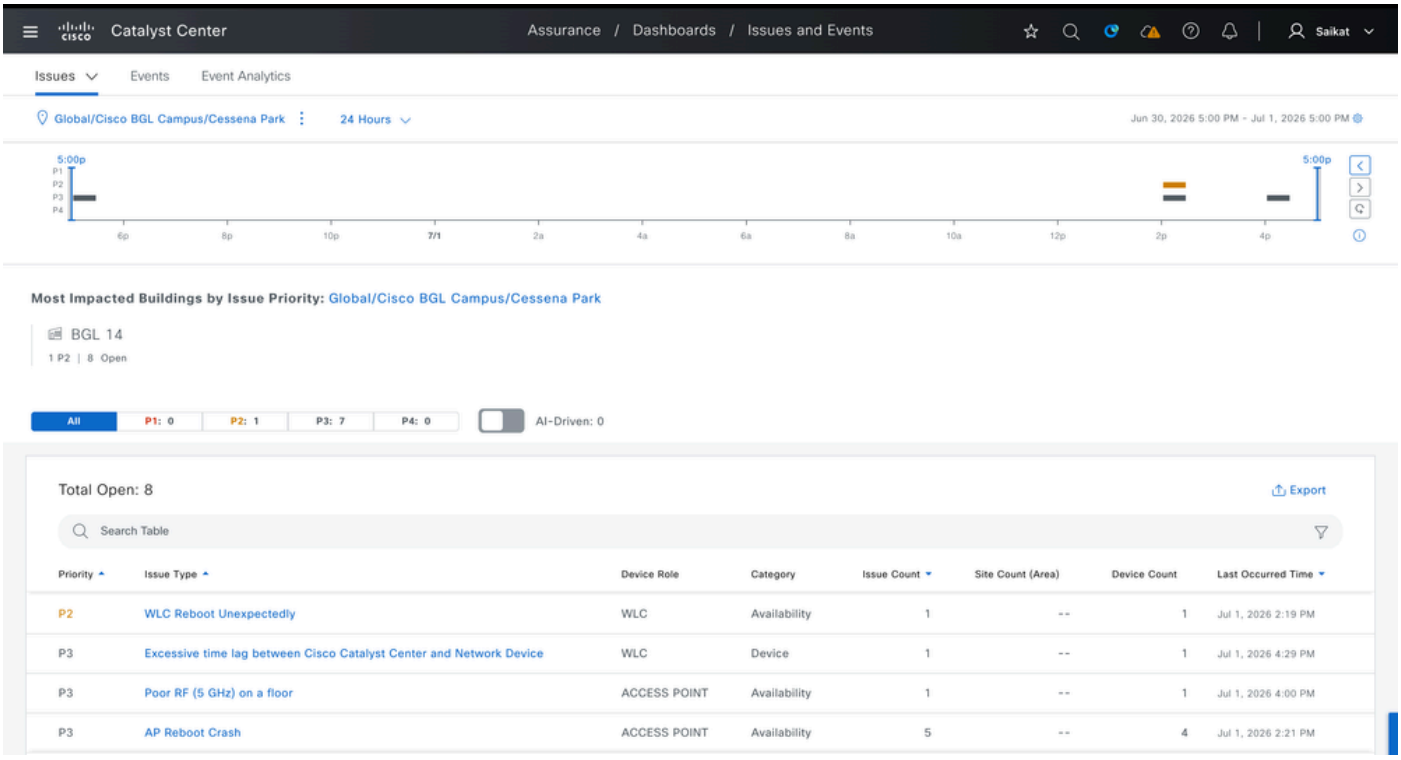
Statistiques WLC sur Catalyst Center

Comme tout cela est corrélé, vous pouvez corréler plusieurs facteurs connexes au moment de l'émission et obtenir une compréhension claire. Avec ces statistiques, vous ne pouvez pas exactement obtenir la cause première du problème, mais nous pouvons éliminer toutes les causes potentielles qui peuvent nous aider à dépanner plus loin et à configurer le type de journaux requis pour être collectés en temps réel.

Problème avec un point d'accès

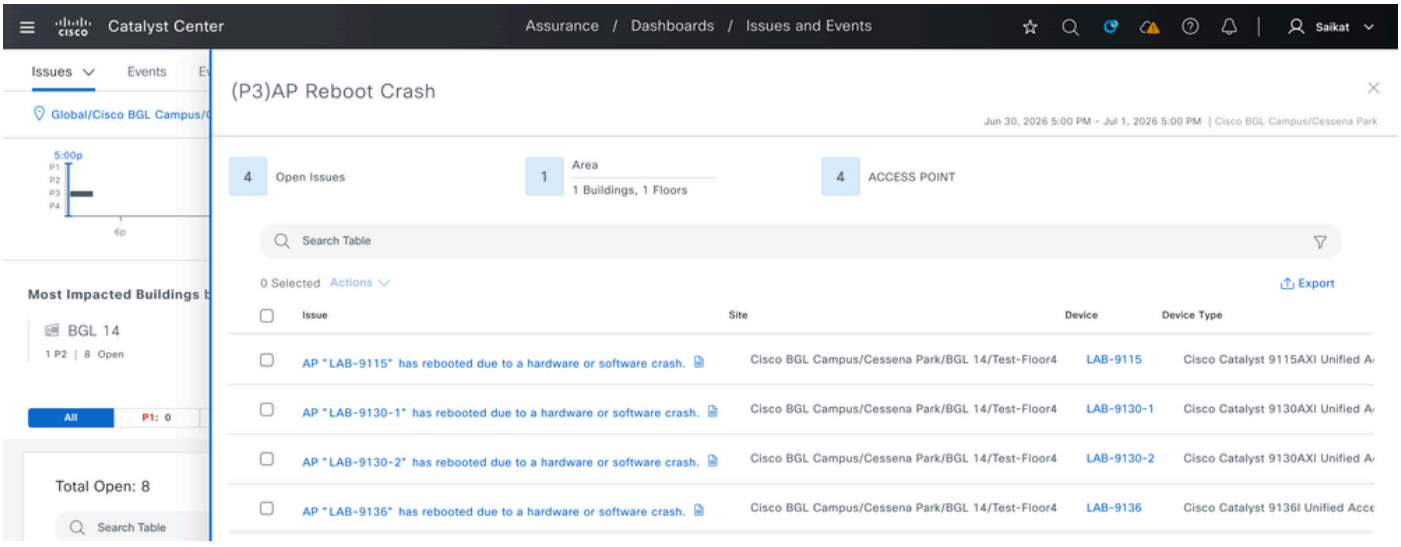
Lorsqu'un point d'accès Cisco rencontre des problèmes tels que des événements de déconnexion,

des anomalies d'état radio, des redémarrages, des pannes, de mauvaises conditions RF, une utilisation élevée du canal ou une inactivité, Catalyst Center génère des alertes avec les niveaux de priorité appropriés. Vous pouvez afficher ces alertes en accédant à Assurance > Issues and Health Settings.



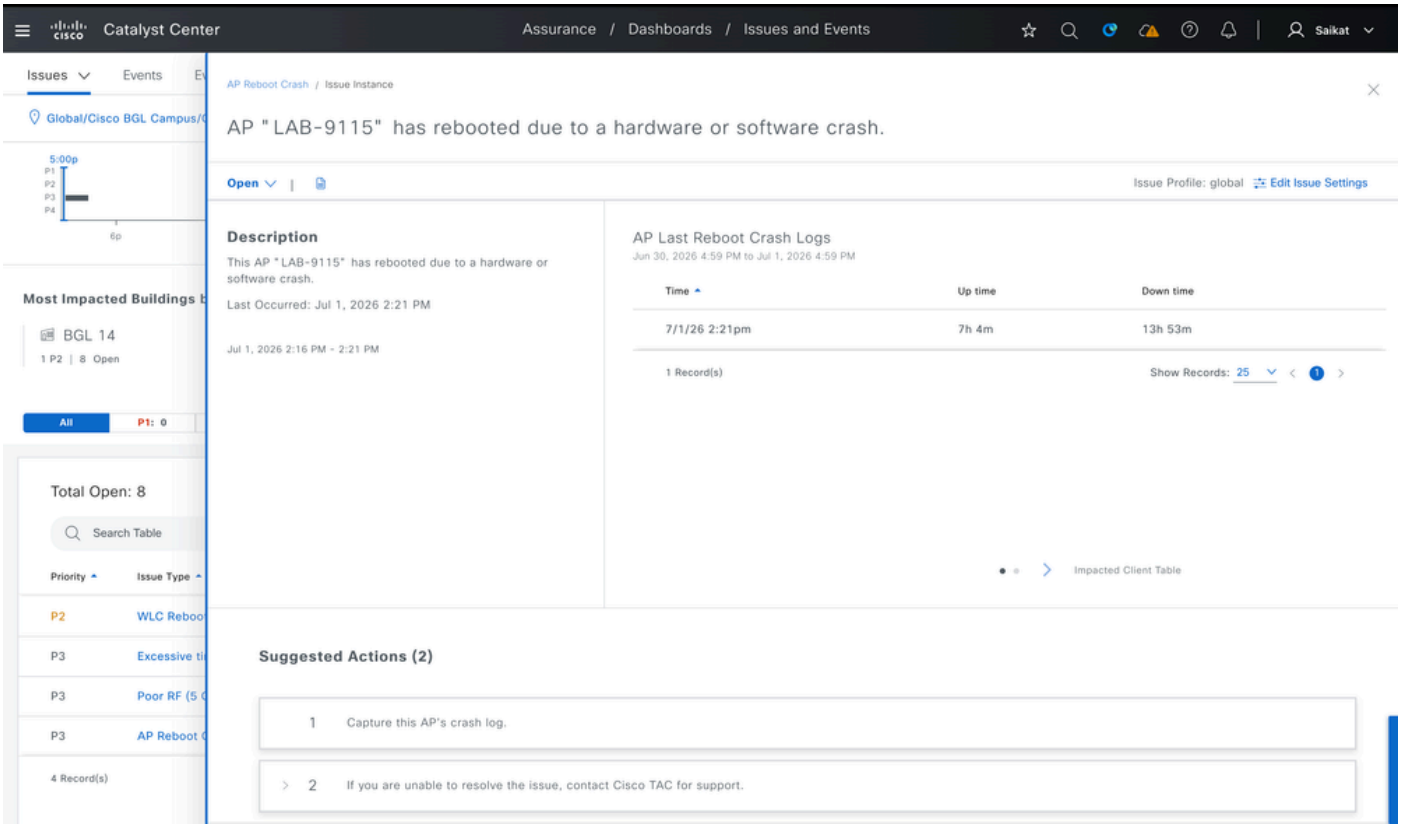
Problèmes signalés Génère des alertes avec une priorité respective

Cette section affiche tous les problèmes en cours dans votre environnement. En cliquant sur des événements individuels, vous pouvez obtenir des informations détaillées en cliquant sur chaque événement individuellement :



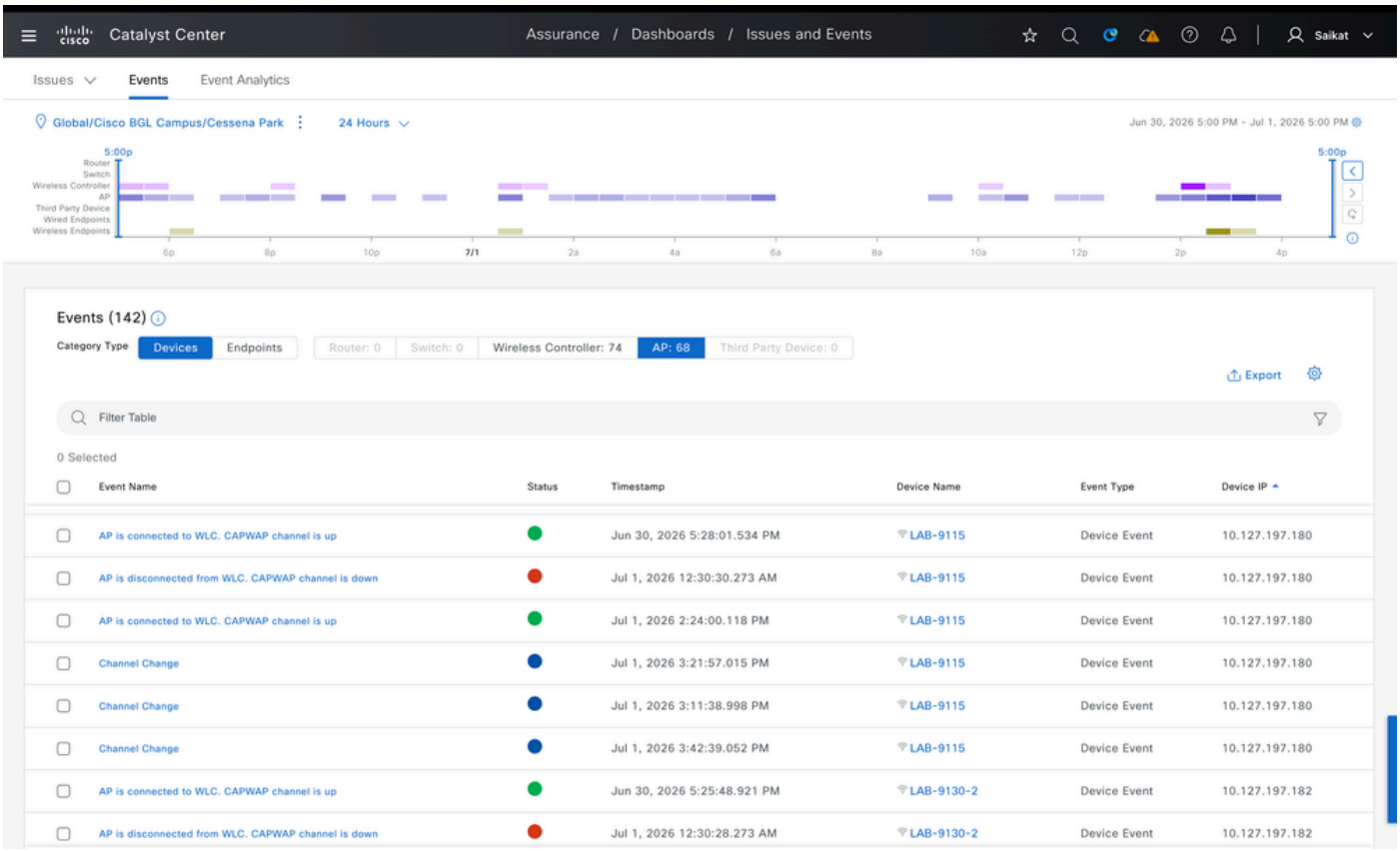
Présentation détaillée des problèmes signalés

En cliquant sur un problème spécifique, vous pouvez afficher des informations détaillées le concernant, ainsi que des suggestions d'actions pour le résoudre ou approfondir l'enquête.

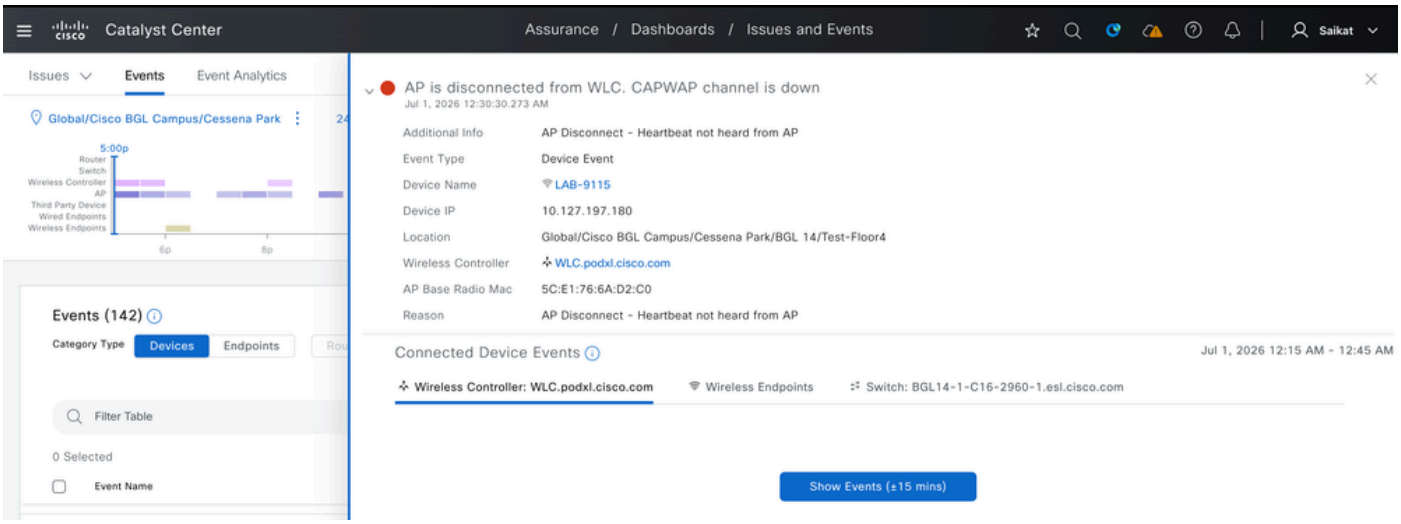


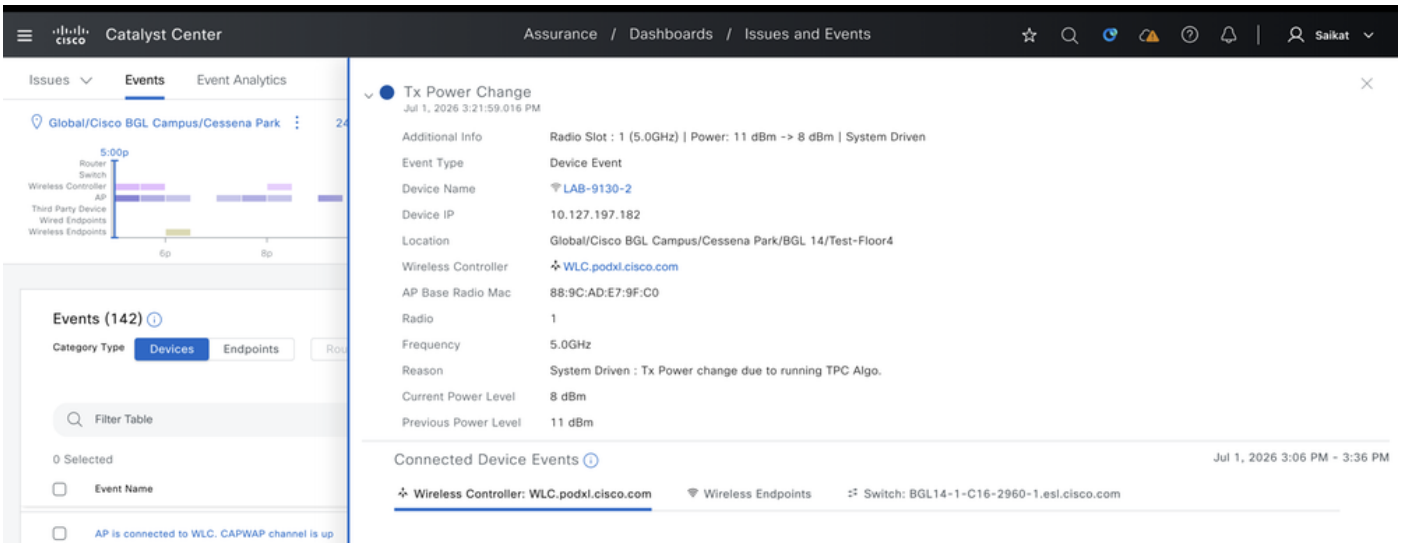
Action suggérée pour le problème signalé sur le point d'accès

En outre, vous pouvez accéder à l'Observateur d'événements, qui contient tous les événements reçus par Catalyst Center en tant que syslogs. Cela est utile pour suivre tous les événements tels que l'activité de jonction/disjonction AP, les changements de canal, les modifications de puissance TX et les redémarrages. Ces événements sont capturés à la fois pour le contrôleur sans fil et les points d'accès individuels.

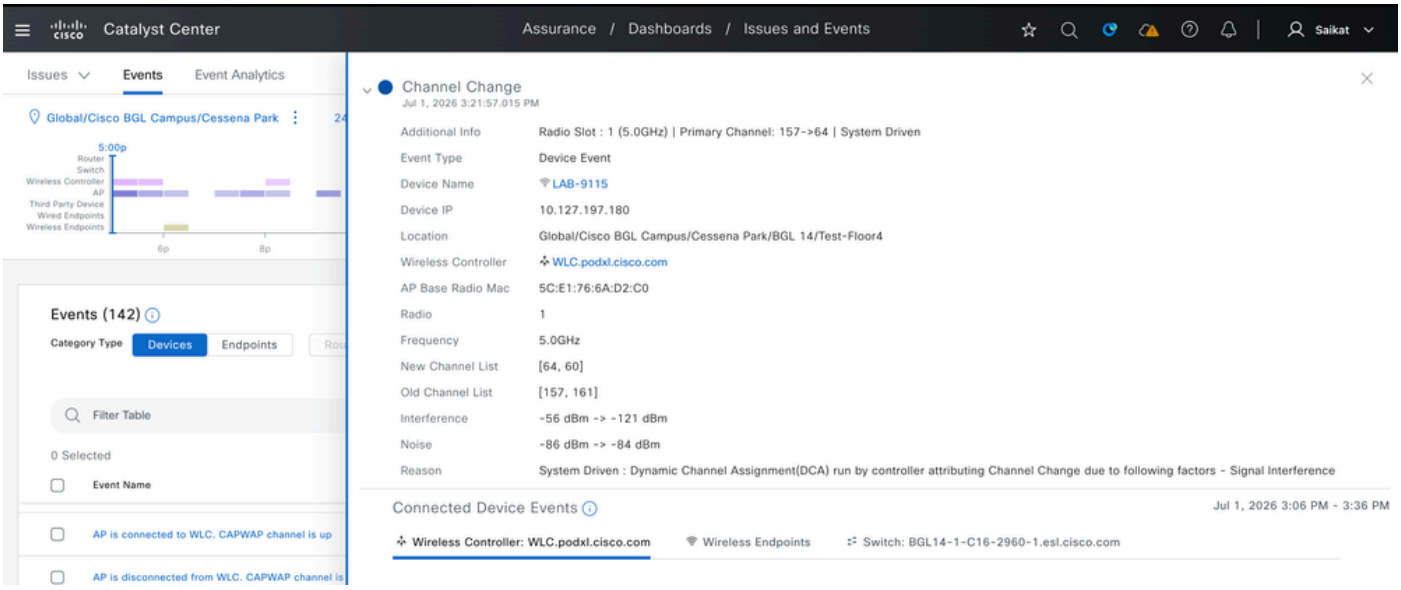


Observateur d'événements pour AP sur Catalyst Center

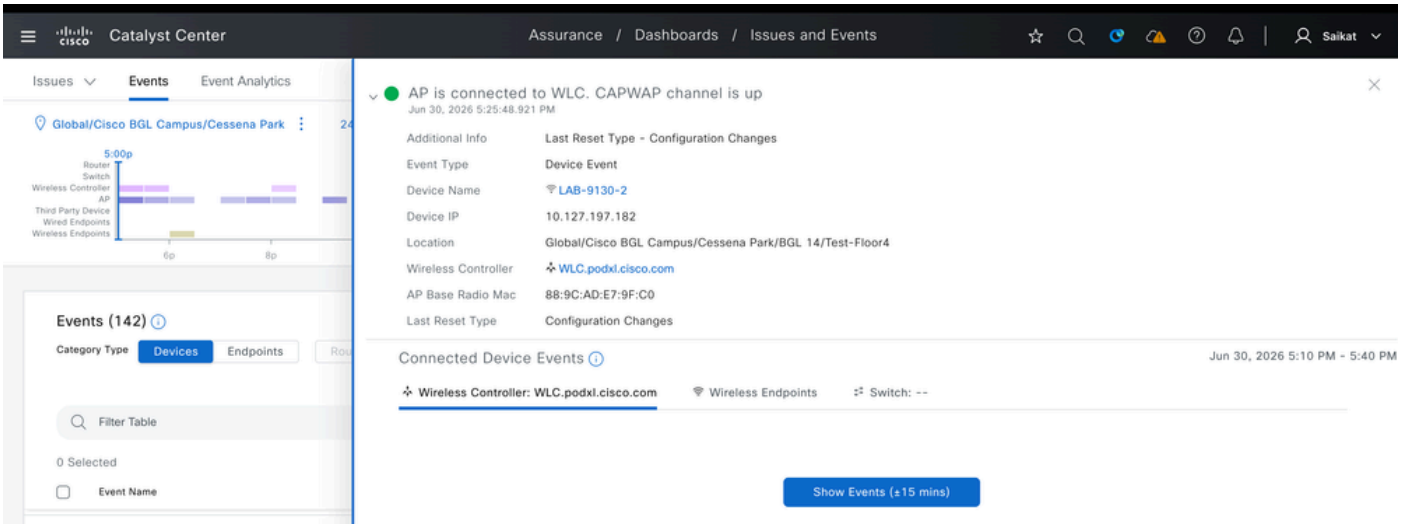




Vue d'ensemble détaillée des événements signalés (avis)

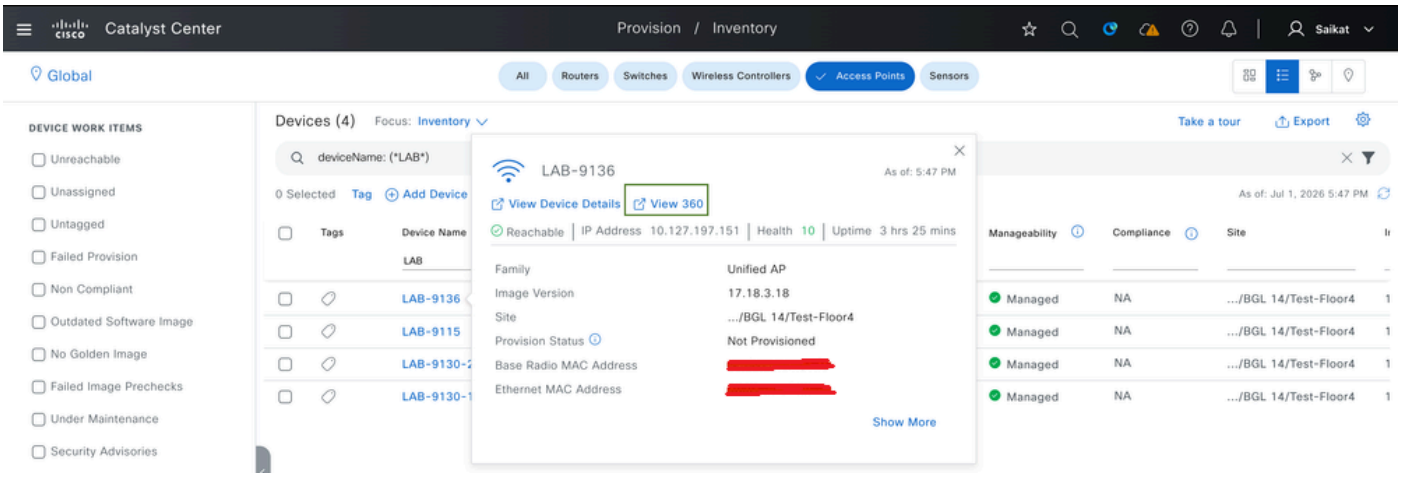


Vue d'ensemble détaillée des événements signalés (avis)



Vue d'ensemble détaillée des événements signalés (Info)

Pour les problèmes spécifiques à un point d'accès individuel, vous pouvez vérifier la vue 360 Health pour ce périphérique. Vous pouvez voir ici l'état d'accessibilité, les événements et les problèmes signalés, ainsi que le score d'intégrité pour ce point d'accès à un moment donné. Le score d'intégrité est calculé en fonction de l'utilisation de la mémoire, de l'utilisation des canaux, de la qualité de l'air, des interférences et du trafic. Pour cela, naviguez vers Provisionner > Inventaire > Point d'accès > AP :

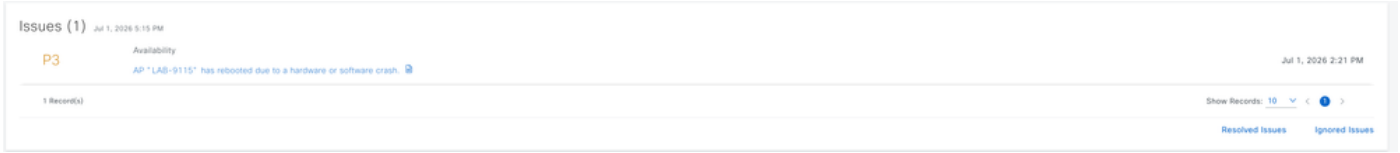


Récapitulatif de télémétrie du périphérique 360 : Vous pouvez voir ici la chronologie du score d'intégrité global des points d'accès, l'utilisation des ressources système (mémoire, CPU), les erreurs de liaison du plan de données et les statistiques spécifiques à la radio (bruit, utilisation du canal, interférences, utilisation du trafic) pour les deux radios. Le périphérique 360 vous permet de déplacer le curseur de chronologie de l'état vers n'importe quel point de la fenêtre historique prise en charge (30 jours).



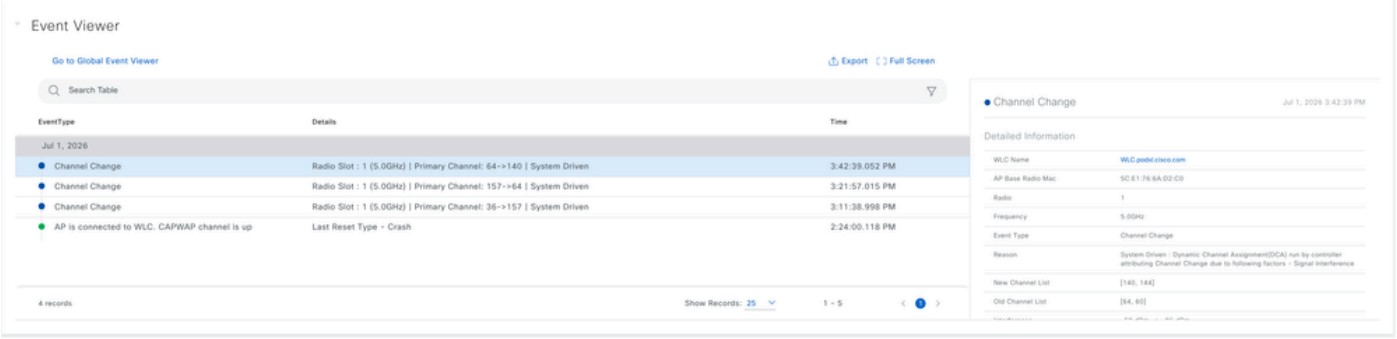
Affichage 360 : État et état de la télémétrie AP

Problèmes - Ici, vous pouvez voir la liste des problèmes ouverts pour le point d'accès, ainsi que la gravité (P1-P4), la catégorie de problème, la description et les horodatages.



Problème signalé pour AP

Observateur d'événements - Vous pouvez voir un journal chronologique des événements AP (par exemple les changements de canal, l'état CAPWAP) ainsi que des informations d'événements détaillées telles que le nom du WLC, la radio, la fréquence, la raison et les listes de canaux anciens/nouveaux.



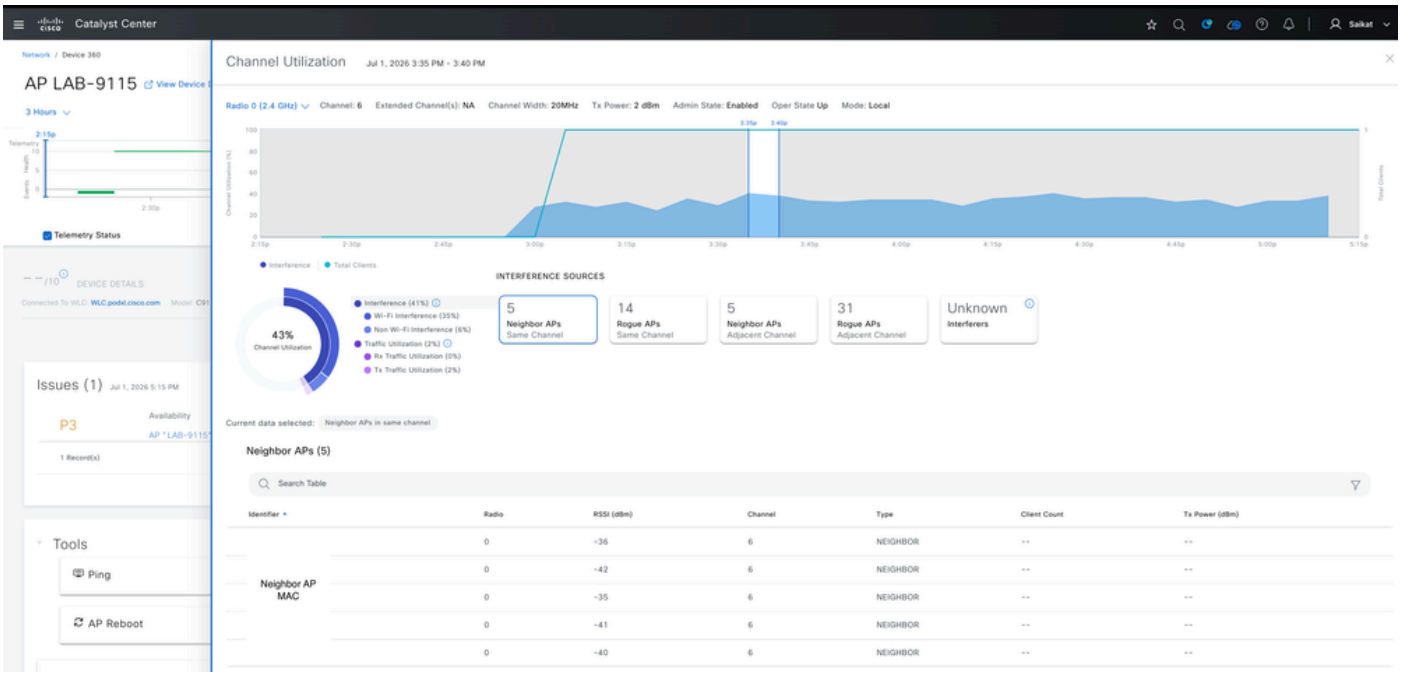
Observateur d'événements de chaque point d'accès

Topologie de voisinage physique avec liste de clients : cette vue affiche la topologie physique connectant le WLC, le point d'accès et les clients connectés, ainsi que des détails supplémentaires sur le client, tels que le nom du périphérique, le score d'intégrité et l'indicateur de ligne de commande.



Topologie physique du point d'accès

Utilisation des canaux : vous pouvez voir la tendance d'utilisation des canaux des points d'accès, les sources d'interférence (points d'accès voisins, points d'accès non autorisés, interféreurs inconnus) et une table détaillée des points d'accès voisins avec RSSI, canal et type.



Utilisation des canaux pour chaque point d'accès

Informations détaillées (onglet Périphérique) - Cette section présente des informations sur le périphérique (nom du point d'accès, IP, modèle, adresses MAC, version du logiciel), des détails sur la disponibilité (temps de disponibilité, temps de jonction du contrôleur, raison de la dernière réinitialisation), des graphiques d'utilisation du processeur/de la mémoire et le tableau de connectivité point d'accès/WLC.



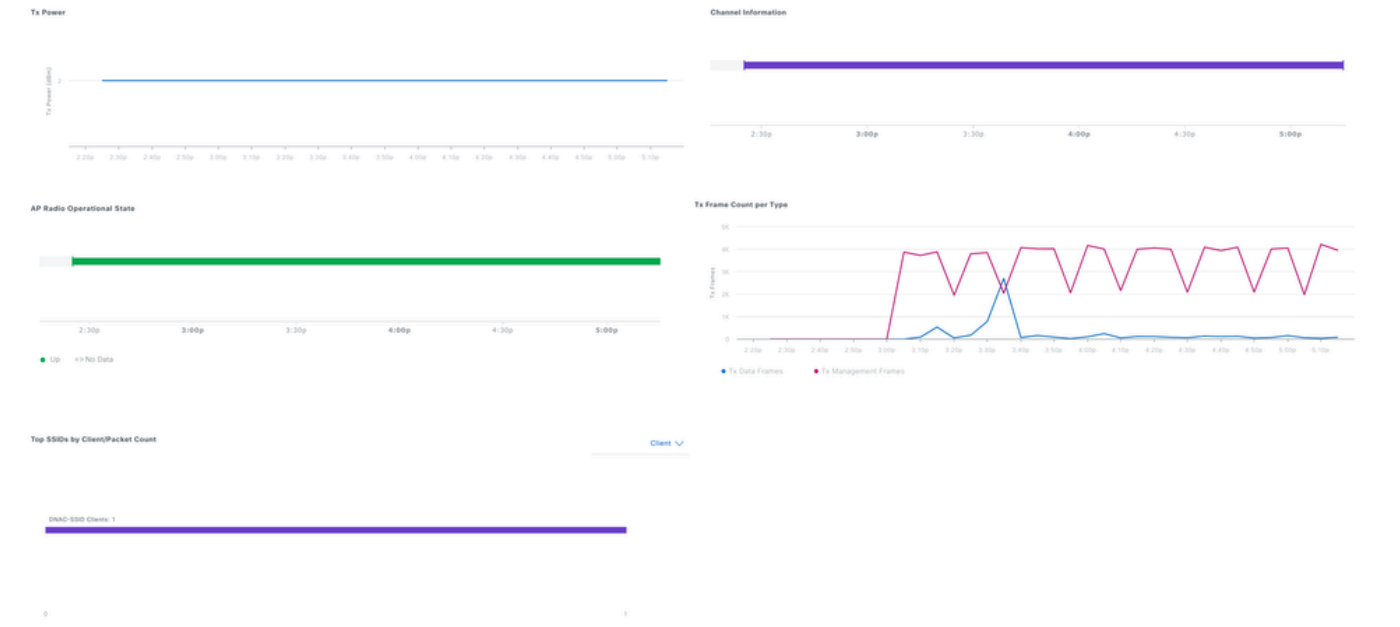
Détails du périphérique pour AP

ICP spécifiques à la radio : Vous pouvez afficher ici les indicateurs de performance clés de niveau radio, notamment l'utilisation du canal, le nombre de clients, le débit (Rx/Tx), les tentatives, le bruit et la qualité de l'air pour la radio sélectionnée.

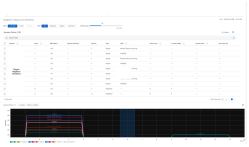


Statistiques RF pour chaque point d'accès

Puissance Tx, Informations sur les canaux et statistiques de trames : Sur cet écran, vous pouvez voir les tendances de puissance Tx, l'historique d'attribution des canaux, l'état opérationnel de la radio AP, le nombre de trames Tx par type (données par rapport à gestion) et les principaux SSID par client/nombre de paquets.



Statistiques RF pour chaque point d'accès

Voisins, intrus et intrus : Cette vue vous permet de voir tous les périphériques voisins, indésirables et sources d'interférence avec leur RSSI, les canaux affectés, le SSID, le nombre de clients, la puissance Tx et l'indice de gravité, ainsi qu'un graphique RSSI-vs-channel visuel. 

Rogue, Neighbor et Interferers signalés pour chaque point d'accès

Le tableau de bord du périphérique 360 rassemble des détails RF tels que l'utilisation du canal, les interférences, le bruit et les tentatives, ainsi que des informations sur les voisins, les éléments indésirables et les éléments interférents à proximité, ce qui vous aide à déterminer si un problème de point d'accès est causé par un encombrement RF, des conflits de canaux ou des éléments indésirables. Les données d'état des périphériques, telles que le processeur, la mémoire, l'historique de redémarrage et l'état de connectivité, ainsi que l'Observateur d'événements et le panneau Problèmes, vous aident à comprendre les pannes matérielles, les pertes de connexion et les changements de canal inattendus. Combinée à la topologie et aux vues client, cette vue offre une vue complète du dépannage, des problèmes RF aux problèmes individuels des clients, avec des suggestions d'actions intégrées pour les résoudre

Captures intelligentes pour point d'accès

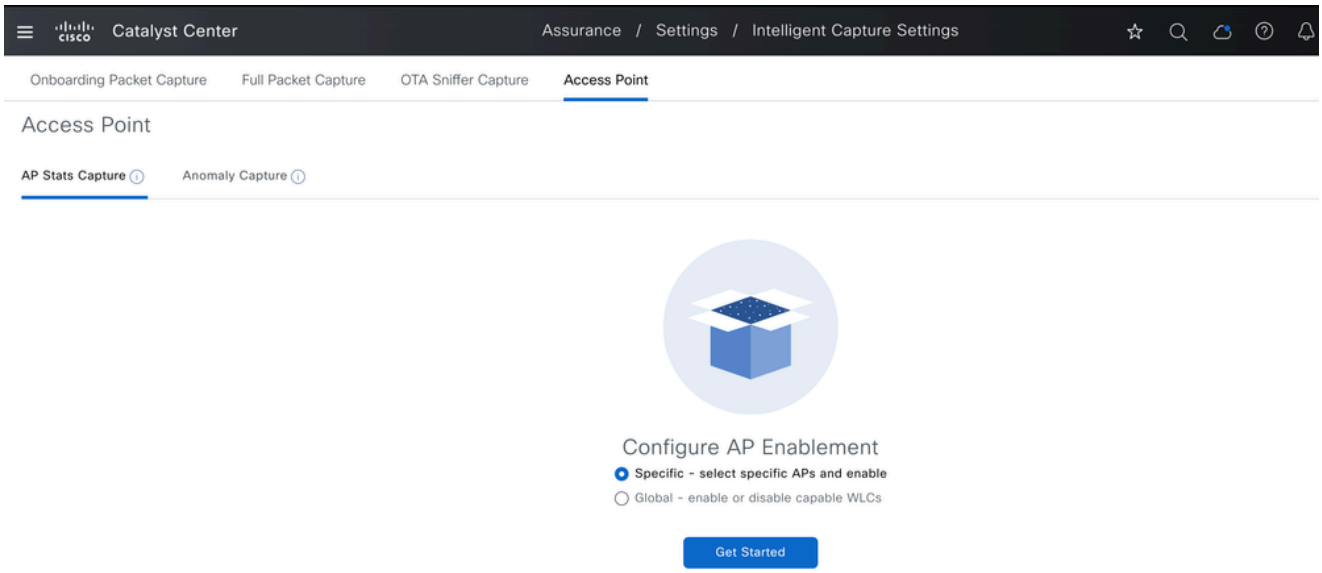
La capture intelligente du point d'accès offre deux fonctionnalités principales : surveillance RF en temps réel permanente, détection des anomalies et capture d'ondes à la demande, analyse spectrale.

Capture de statistiques AP

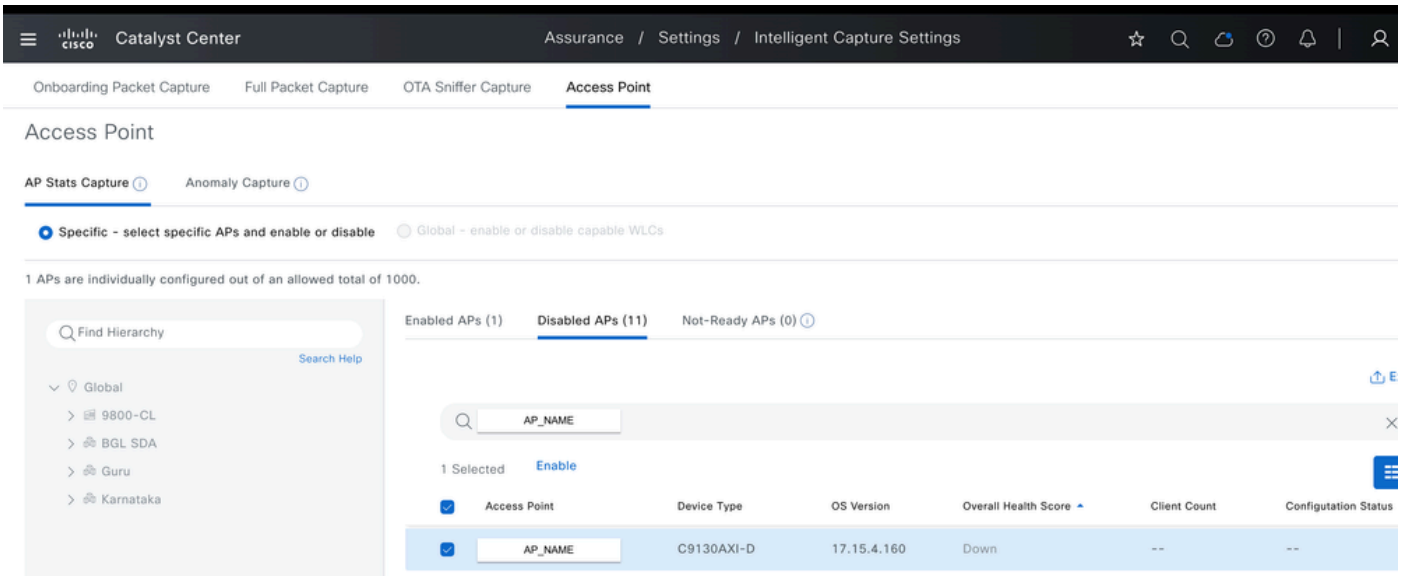
Vous pouvez activer et gérer la collecte de données de statistiques AP pour un ou plusieurs points d'accès, y compris les statistiques radio AP, les statistiques WLAN et les statistiques client AP, avec la prise en charge de 1 000 AP maximum.

Pour activer la capture de statistiques AP, accédez à Assurance > Settings > Intelligent Capture Settings > Access Point > AP Stats Capture. De là, vous avez la possibilité de :

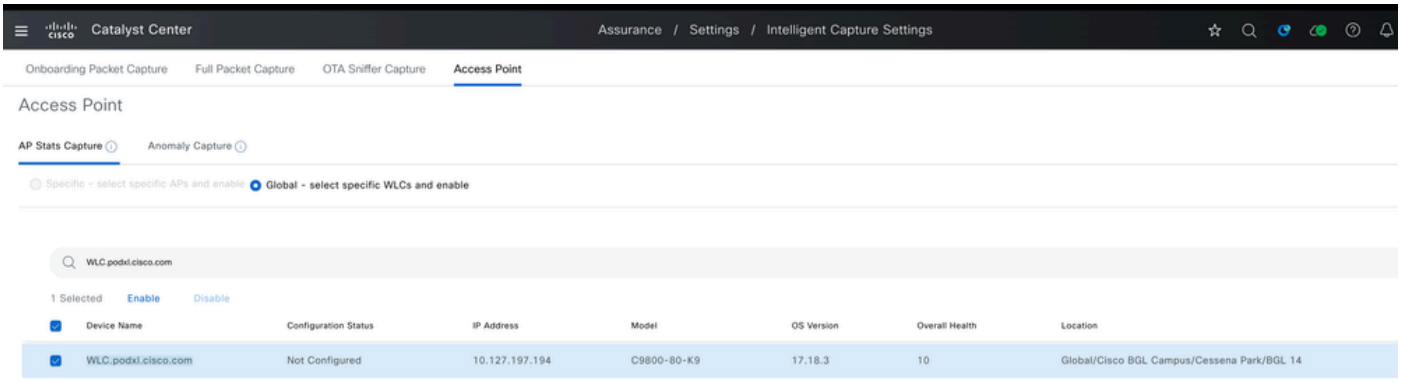
- Activez-le pour des points d'accès spécifiques (jusqu'à 1000) ou
- Activez-le globalement pour tous les AP gérés sous un WLC particulier.



Option de capture de statistiques AP

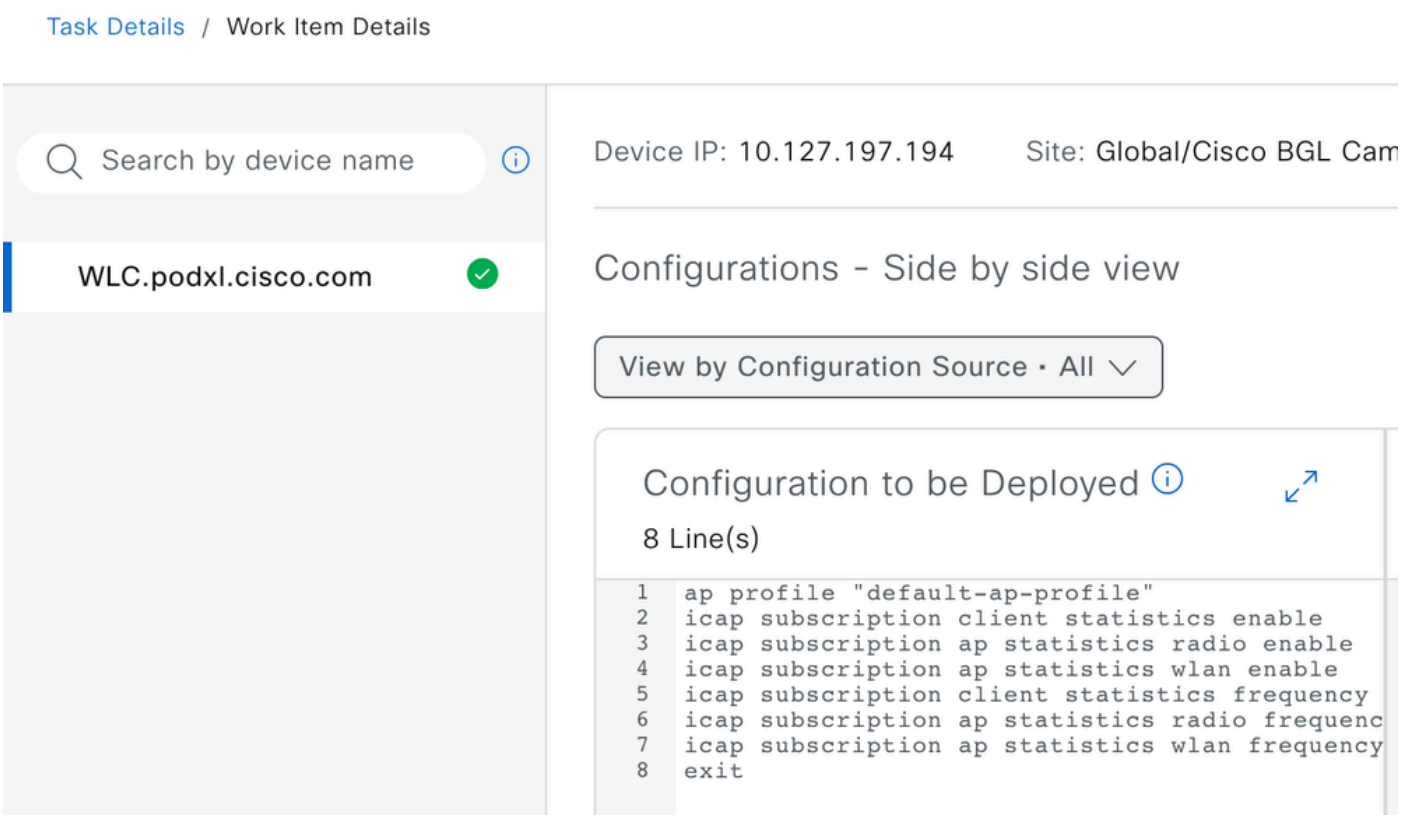


Activer les captures intelligentes de statistiques AP sur un AP spécifique



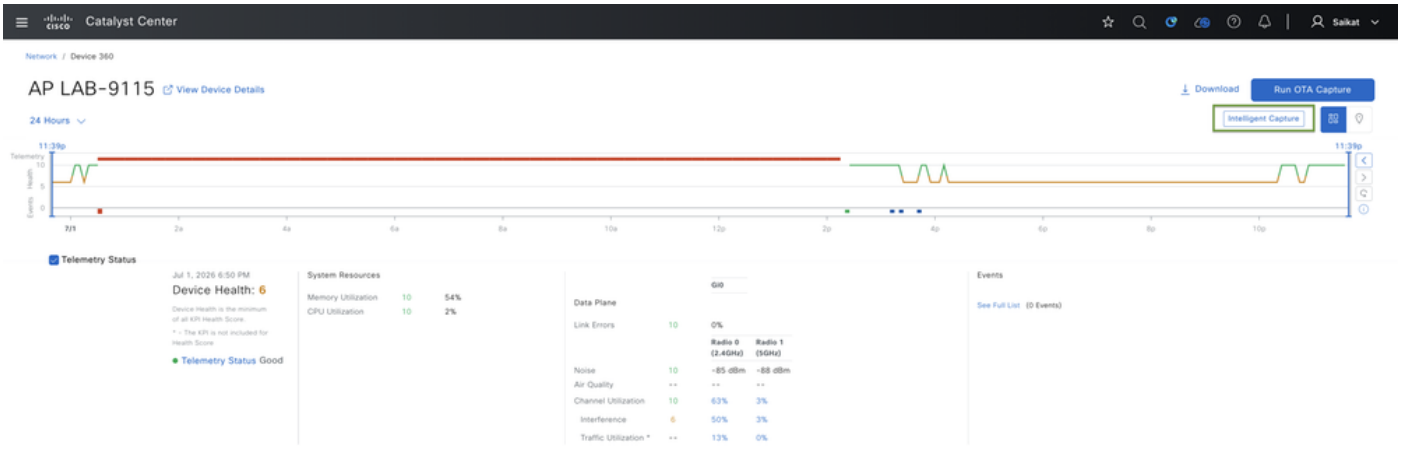
Activer la capture intelligente des statistiques AP globalement

Une fois la capture d'état AP activée, Catalyst Center transmet la configuration correspondante au WLC — soit pour le ou les AP spécifiques sélectionnés, soit pour tous les AP, selon qu'il a été activé au niveau individuel AP ou globalement au niveau WLC.

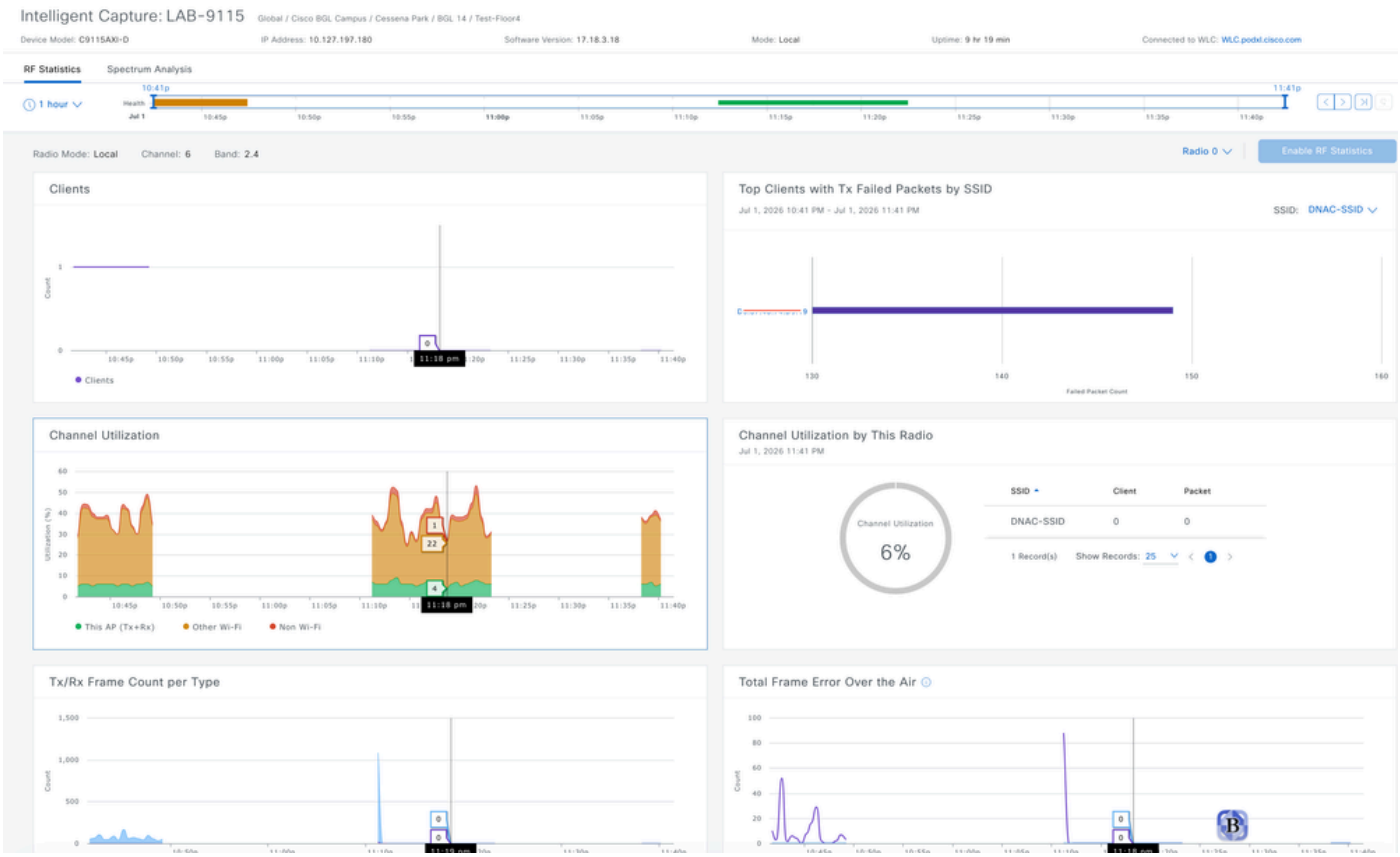


Configuration à transmettre lorsque la capture d'état AP est activée

Après avoir activé cette capture, vous pouvez afficher les données en temps réel collectées via la capture intelligente directement à partir de la page Device 360. En outre, vous pouvez exécuter l'analyse spectrale à la demande pour étudier plus en détail les conditions RF.



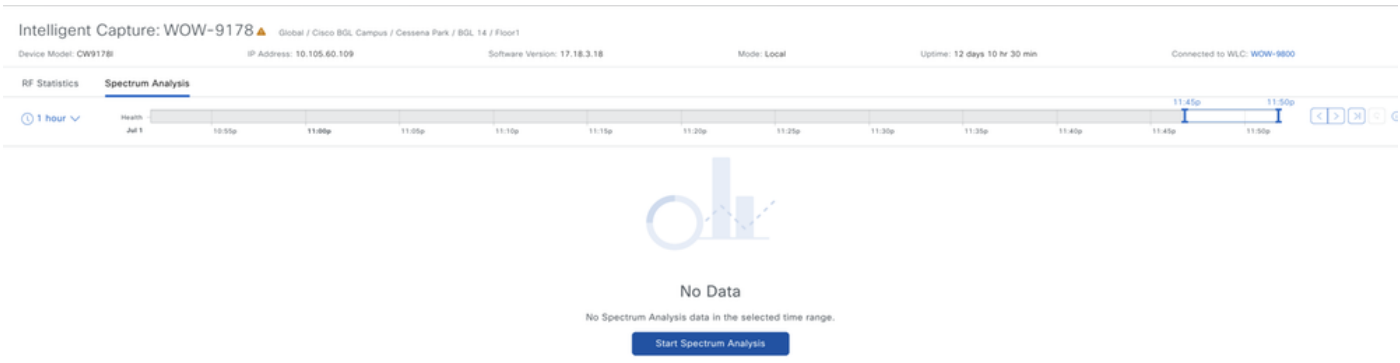
Capture intelligente pour AP dans le périphérique 360



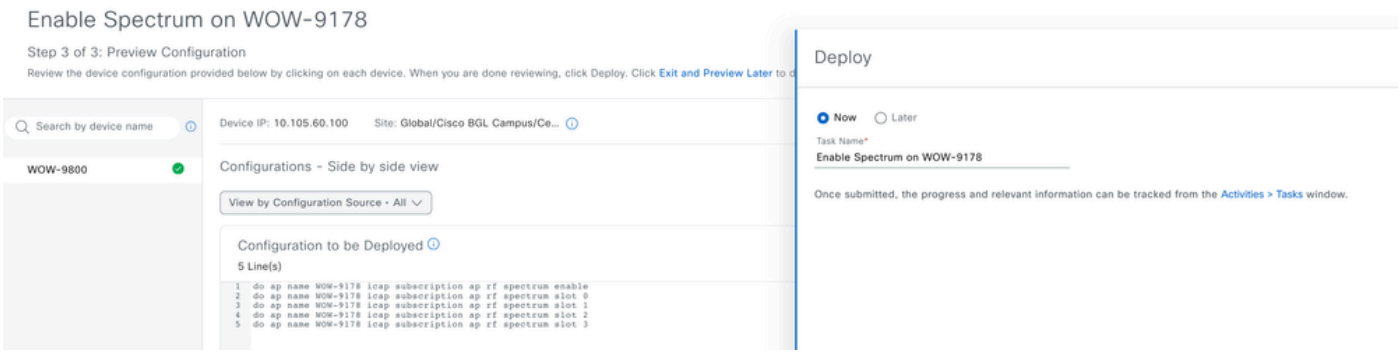
Statistiques AP capturées à l'aide de la capture intelligente sur Catalyst Center

Ici, vous pouvez voir des statistiques en temps réel couvrant le nombre de trames Tx/Rx par type, le nombre total d'erreurs de trames transmises, les compteurs de multidiffusion/diffusion, la puissance Tx et le bruit de fond, l'utilisation des canaux, les principaux clients avec des paquets Tx en panne par SSID et les données client capturées pour un point d'accès spécifique à l'aide de la capture intelligente.

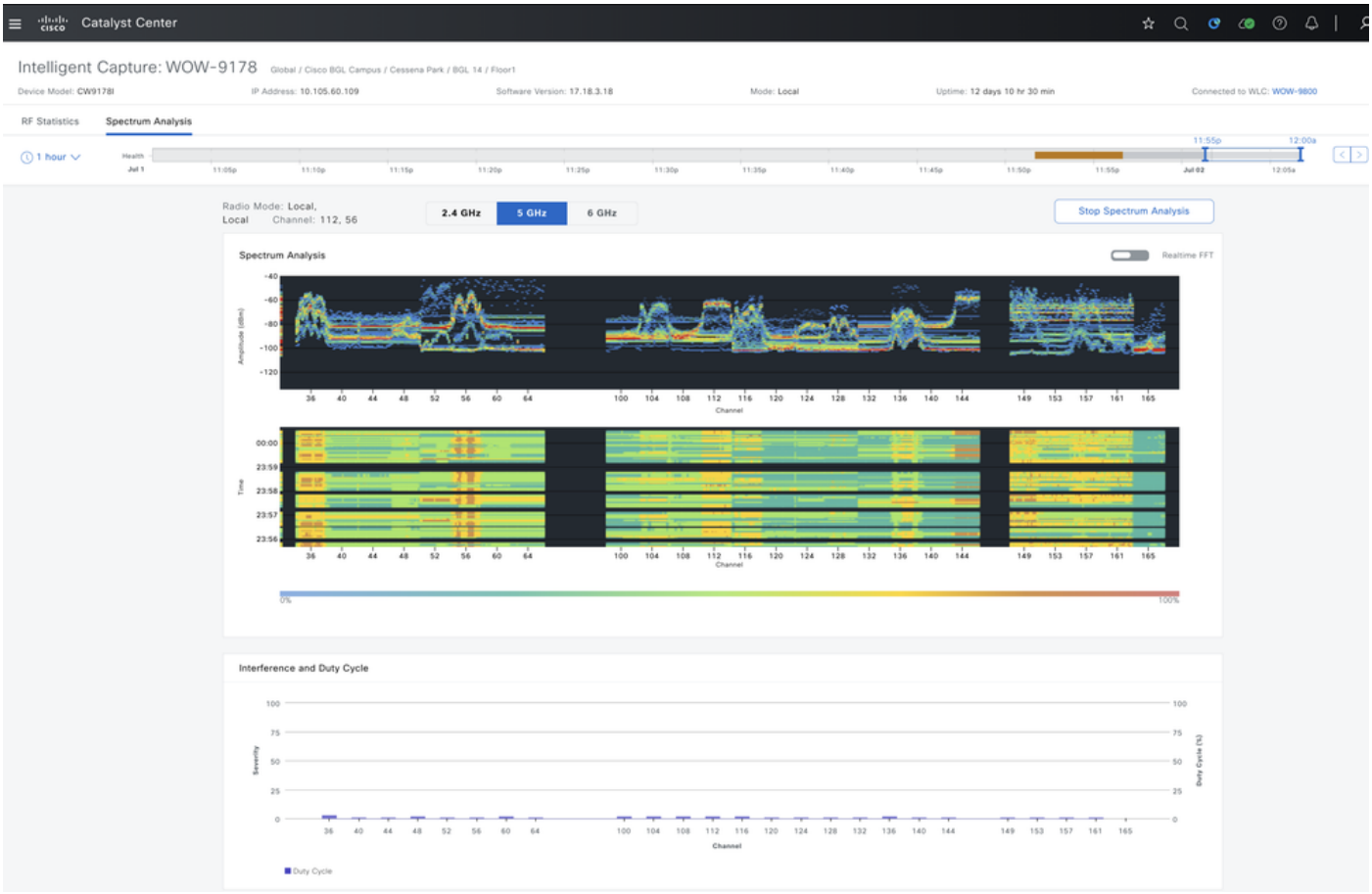
Vous pouvez également exécuter une analyse spectrale à la demande pour un point d'accès individuel chaque fois que nécessaire pour inspecter les conditions RF. Cependant, cette fonctionnalité nécessite le modèle AP pour la prendre en charge.



Analyse Spectrale À La Demande



Configuration appliquée pour l'analyse spectrale



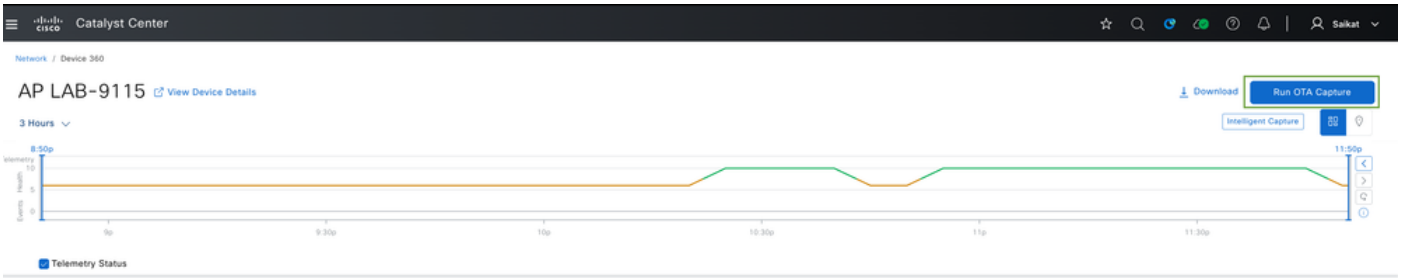
Résultat De L'Analyse Spectrale

Capture de renifleur OTA

Catalyst Center vous permet d'activer OTA Sniffer Capture sur une radio, une bande passante et un canal spécifiques. Une fois activés, tous les paquets de données Wi-Fi circulant sur cette radio et ce canal sont capturés. Vous pouvez sélectionner jusqu'à 2 points d'accès pour effectuer l'analyse. Gardez à l'esprit que les 2 AP configurés pour l'analyse du trafic peuvent passer en mode d'analyse sur leur radio/logement respectif tant que la capture OTA est activée.

Pour l'activer, accédez à Provisionner > Inventaire > Points d'accès, cliquez sur l'AP pour lequel

vous voulez collecter des données OTA, puis sélectionnez Exécuter la capture OTA. Choisissez jusqu'à deux points d'accès proches pour analyser le trafic.

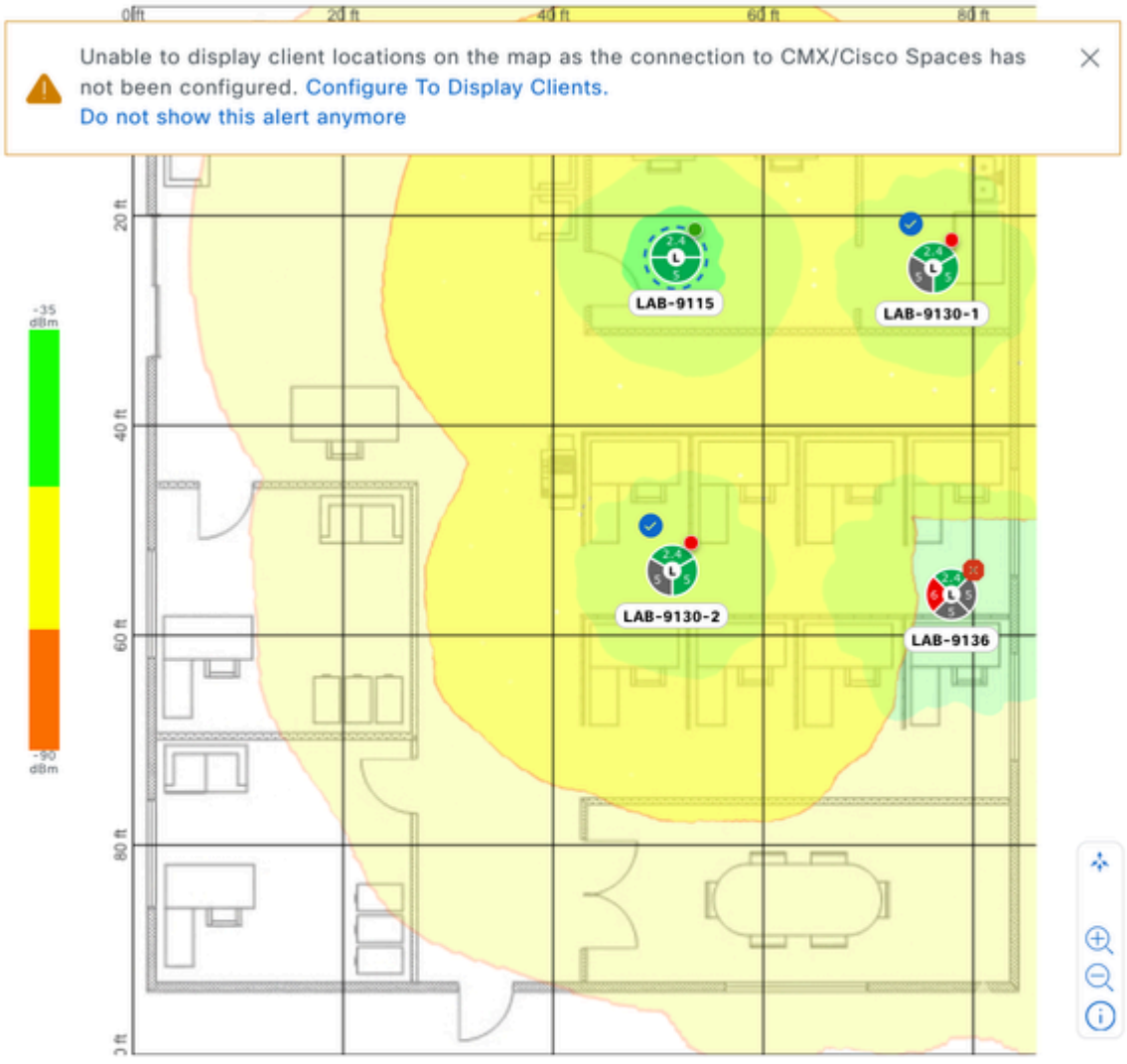


Exécuter la capture OTA sur le point d'accès cible

Run OTA Capture

Select Access Points
This is the Over the Air Sniffer, you can select up to 2 access points. These Access Points will promiscuously sniff the environment.

Global/Cisco BGL Campus/Cessena Park/BGL 14 Test-Floor4



LAB-9130-1 ×

Radios: 0 (2.4 GHz), 1 (5 GHz), 2 (5 GHz)

IP Address: 10.127.197.184

Floor: Test-Floor4

RSSI: -36 dBm

Device 360

LAB-9130-2 ×

Radios: 0 (2.4 GHz), 1 (5 GHz), 2 (5 GHz)

IP Address: 10.127.197.182

Floor: Test-Floor4

RSSI: -36 dBm

Device 360

Cancel Next

Sélection des points d'accès voisins (jusqu'à 2) pour détecter le trafic

Run OTA Capture

Select OTA Sniffer Band, Radio, Channel Width & Channel

LAB-9130-1

MAC Address: 88:9C:AD:1E:19:40

AP LAB-9130-1 supports capturing packets at the radio level.

Select Band
5

Select Radio
1 (Client Count: 0)

Select Channel Width
40

Select Channel
36

LAB-9130-2

MAC Address: 88:9C:AD:E7:9F:C0

AP LAB-9130-2 supports capturing packets at the radio level.

Select Band
5

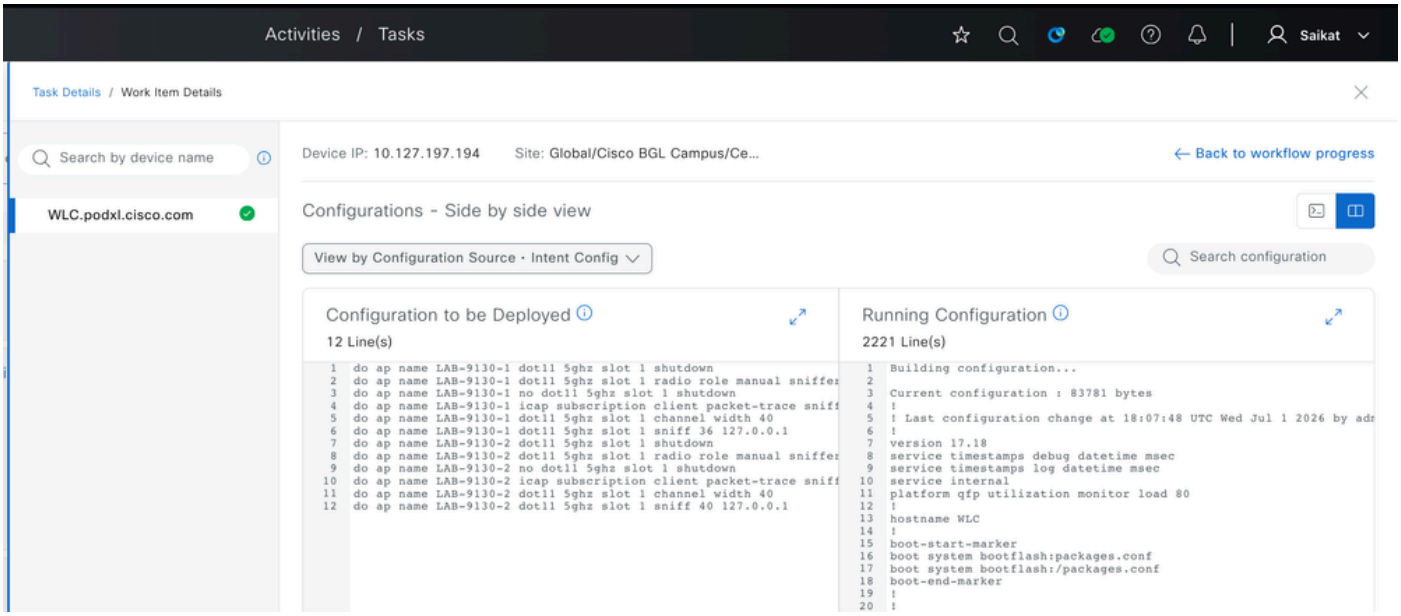
Select Radio
1 (Client Count: 0)

Select Channel Width
40

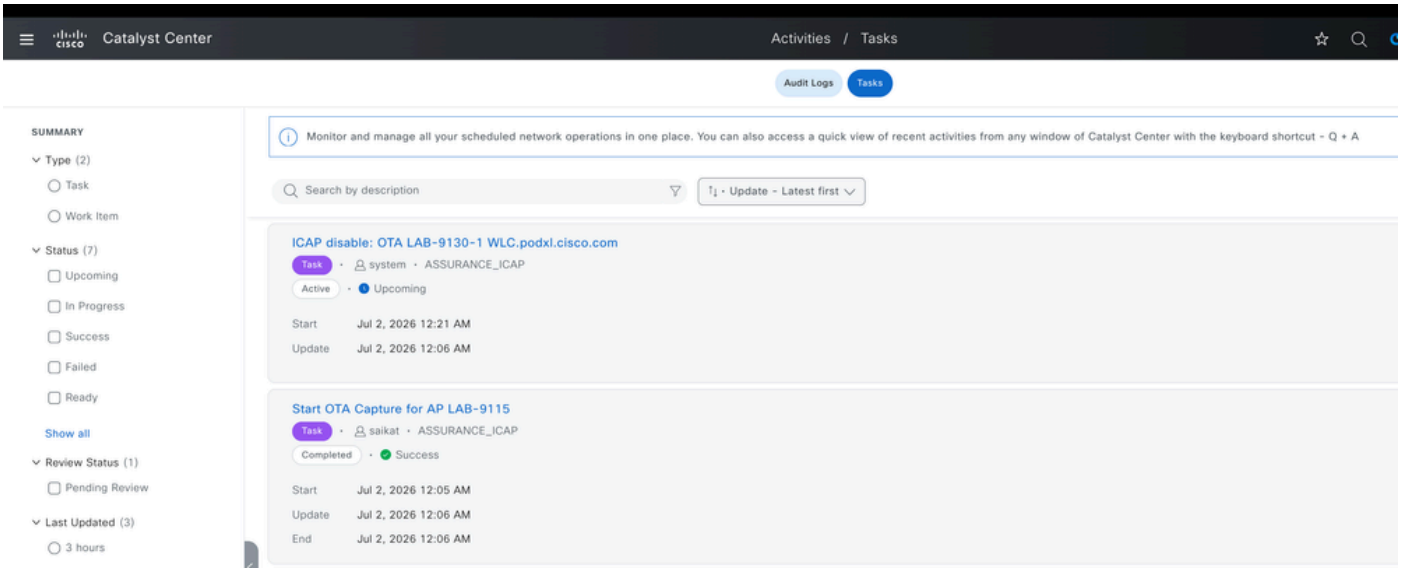
Select Channel
40

back Next

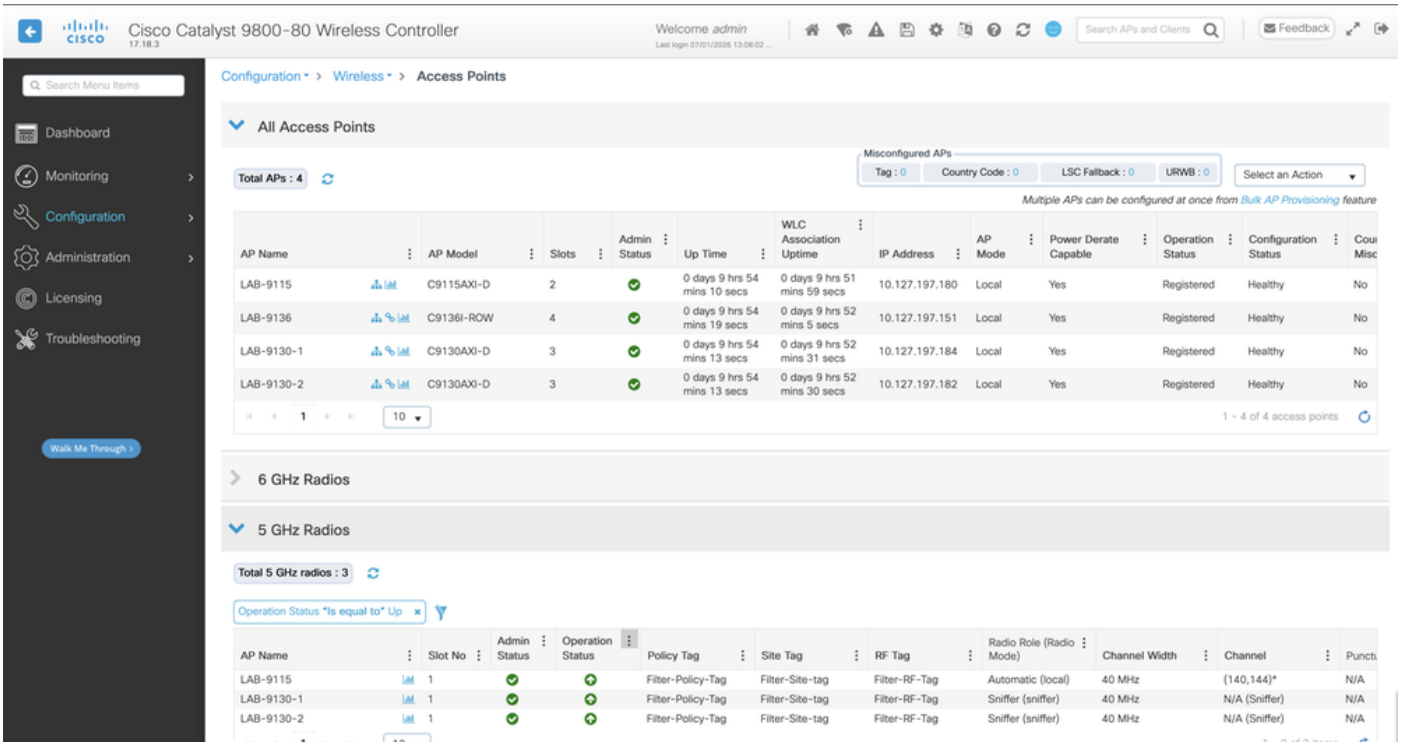
Sélectionnez Radio, Channel-Width, Channel pour détecter le trafic



Aperçu de la configuration pour activer la capture OTA

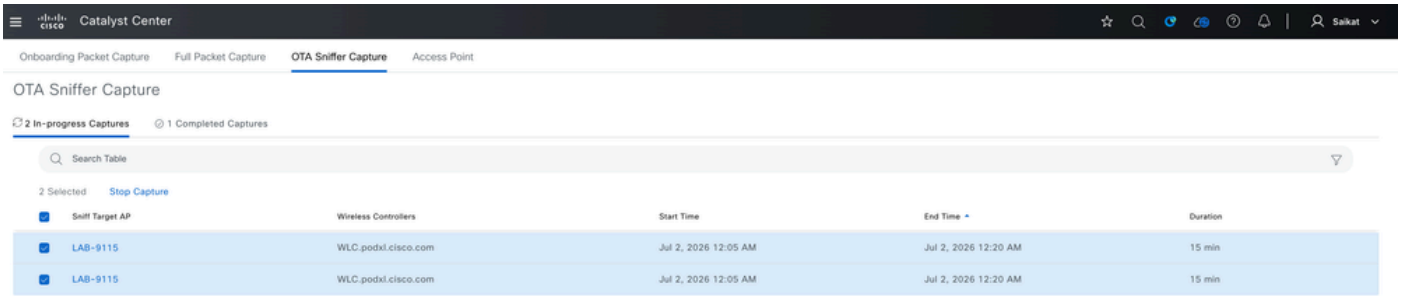


Tâche planifiée lorsque la capture OTA est activée



Emplacement 1 en mode renifleur pour le point d'accès activé pour renifler le trafic

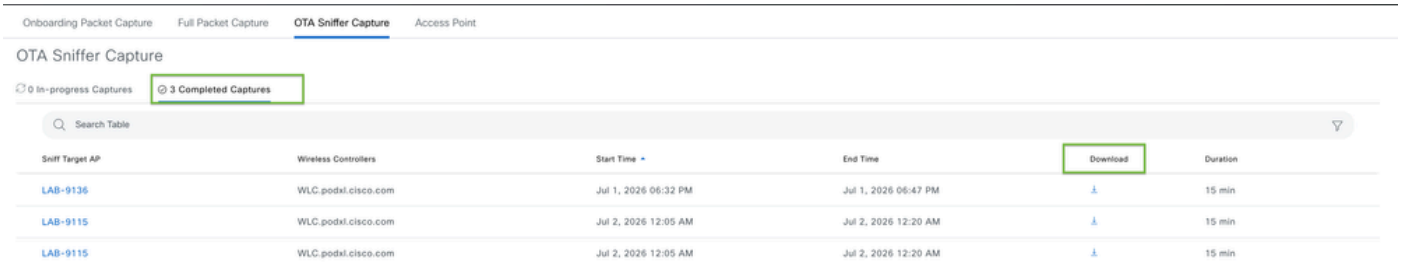
Pour vérifier l'état de l'exécution de la capture OTA, accédez à Assurance > Settings > Intelligent Capture Settings > OTA Sniffer Capture :



État de la capture OTA

Remarque : Par défaut, Catalyst Center exécute cette tâche pendant 15 minutes avant de la désactiver automatiquement, bien qu'elle puisse également être arrêtée manuellement à tout moment.

Une fois la capture OTA terminée, elle apparaît dans la section Captures terminées, à partir de laquelle vous pouvez télécharger le fichier.



Capture terminée - Capture de renifleur OTA

Détection des anomalies

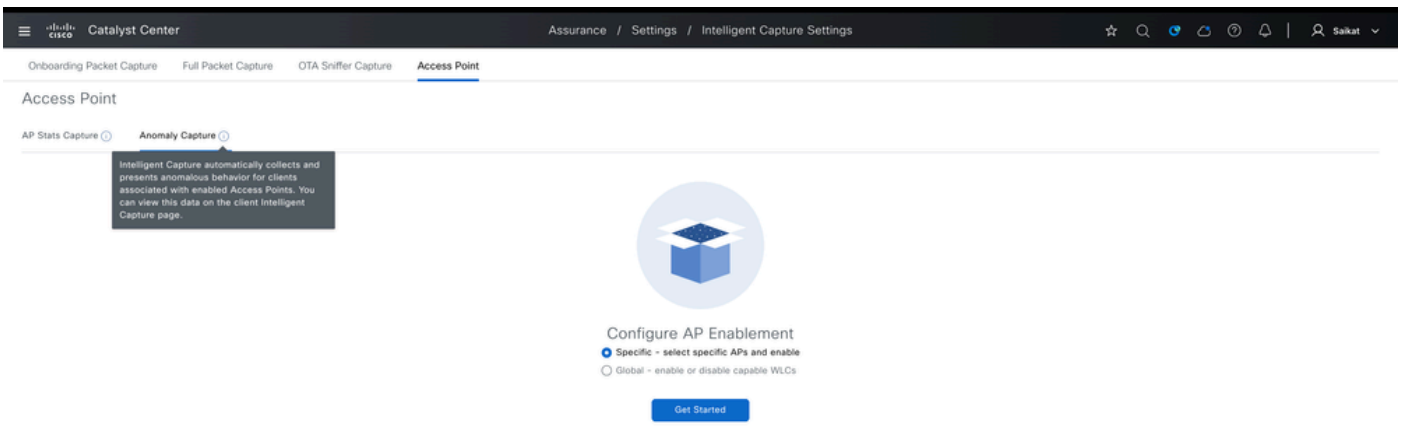
Cette fonctionnalité permet aux points d'accès Cisco de détecter d'éventuelles irrégularités dans le comportement des clients sans fil qui leur sont associés. Il comprend :

- Détection des anomalies
- Capture des paquets anormaux
- Rapports individuels sur les anomalies
- Rapports récapitulatifs des anomalies

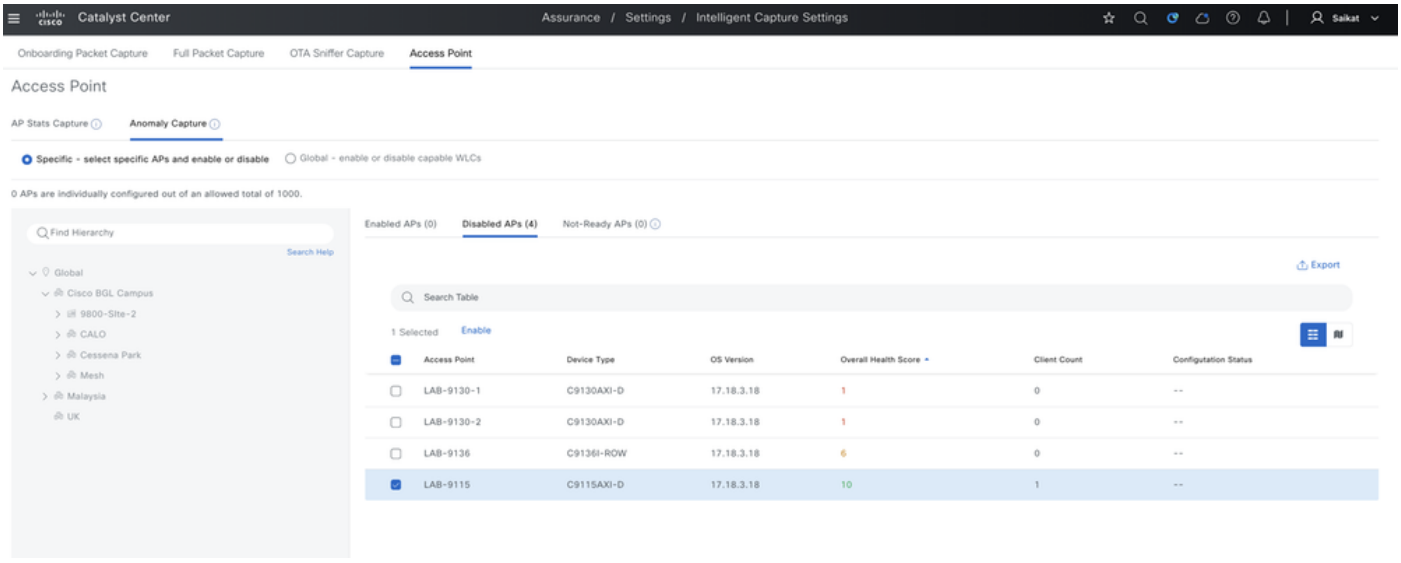
Pour activer la capture d'anomalies AP, accédez à Assurance > Settings > Intelligent Capture Settings > Access Point > Anomaly Capture. De là, vous avez la possibilité de :

- Activez-le pour des points d'accès spécifiques (jusqu'à 1000) ou
- Activez-le globalement pour tous les AP gérés sous un WLC particulier.

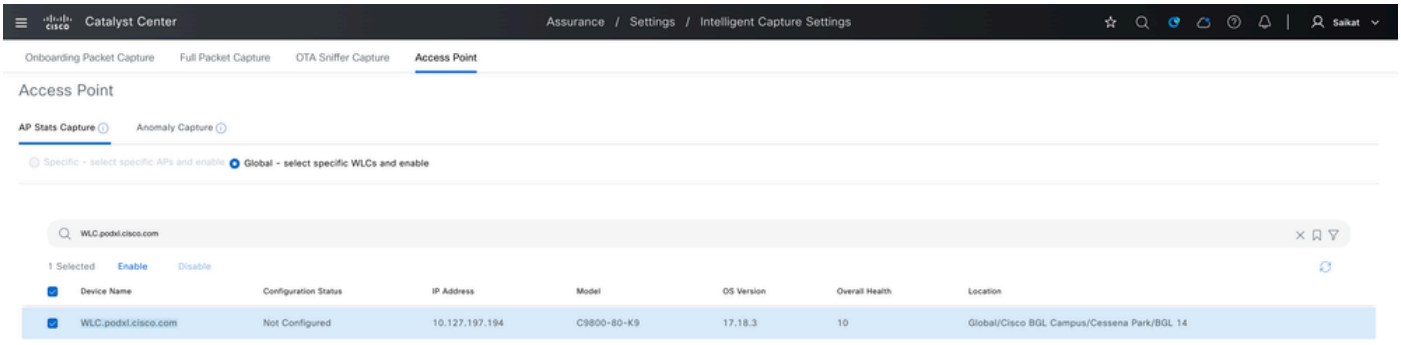
Une fois activée, la capture intelligente collecte et présente automatiquement un comportement anormal pour les clients associés à ces points d'accès. Ces données peuvent être affichées sur la page Capture intelligente du client.



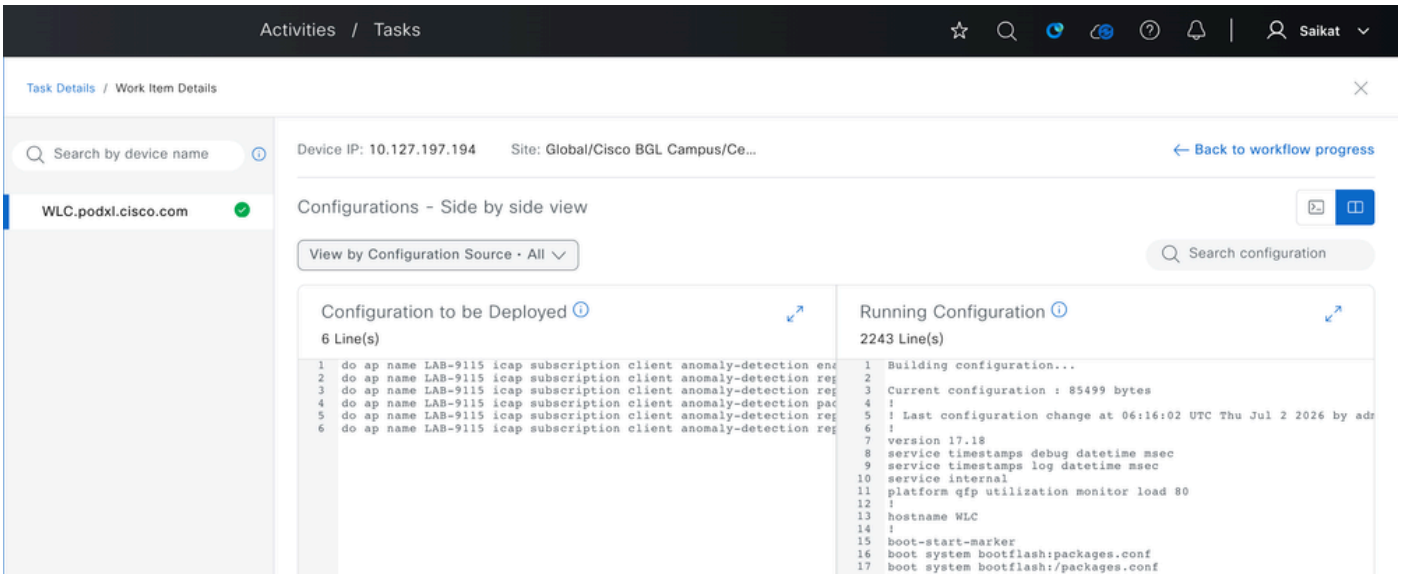
Configurer la capture des anomalies



Activer la capture d'anomalies pour un point d'accès spécifique

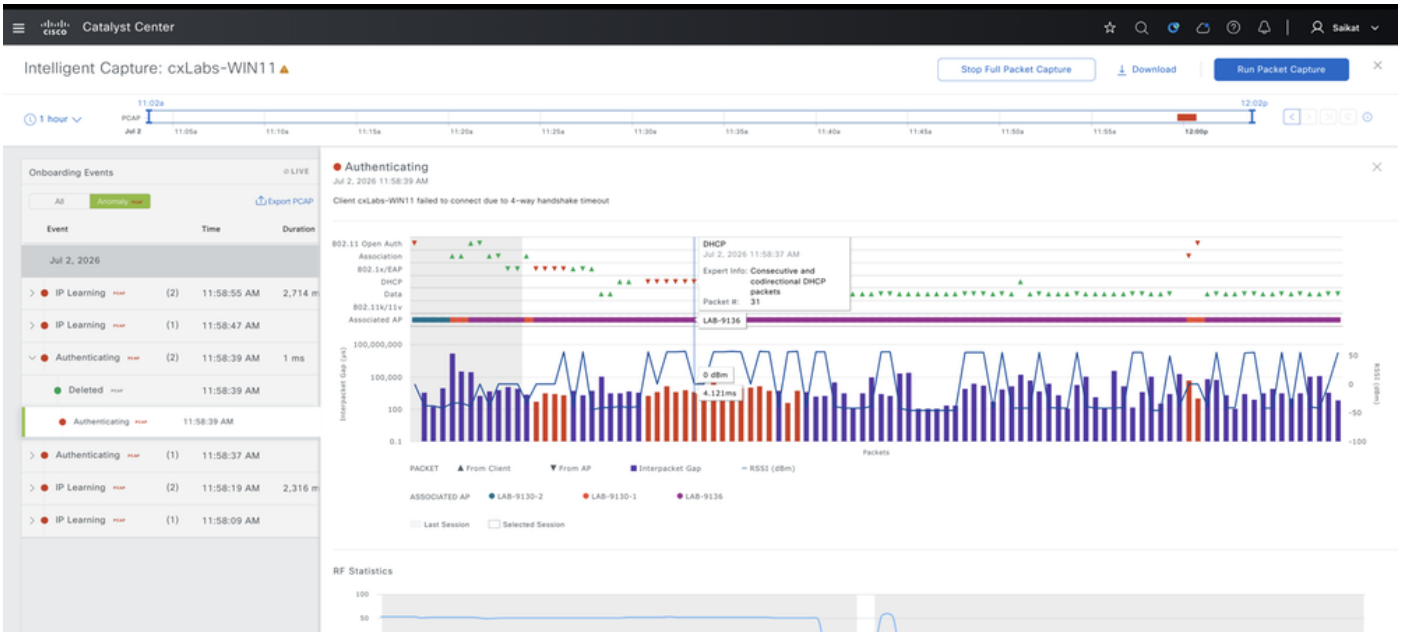


Activer la capture d'anomalie globale pour un WLC spécifique

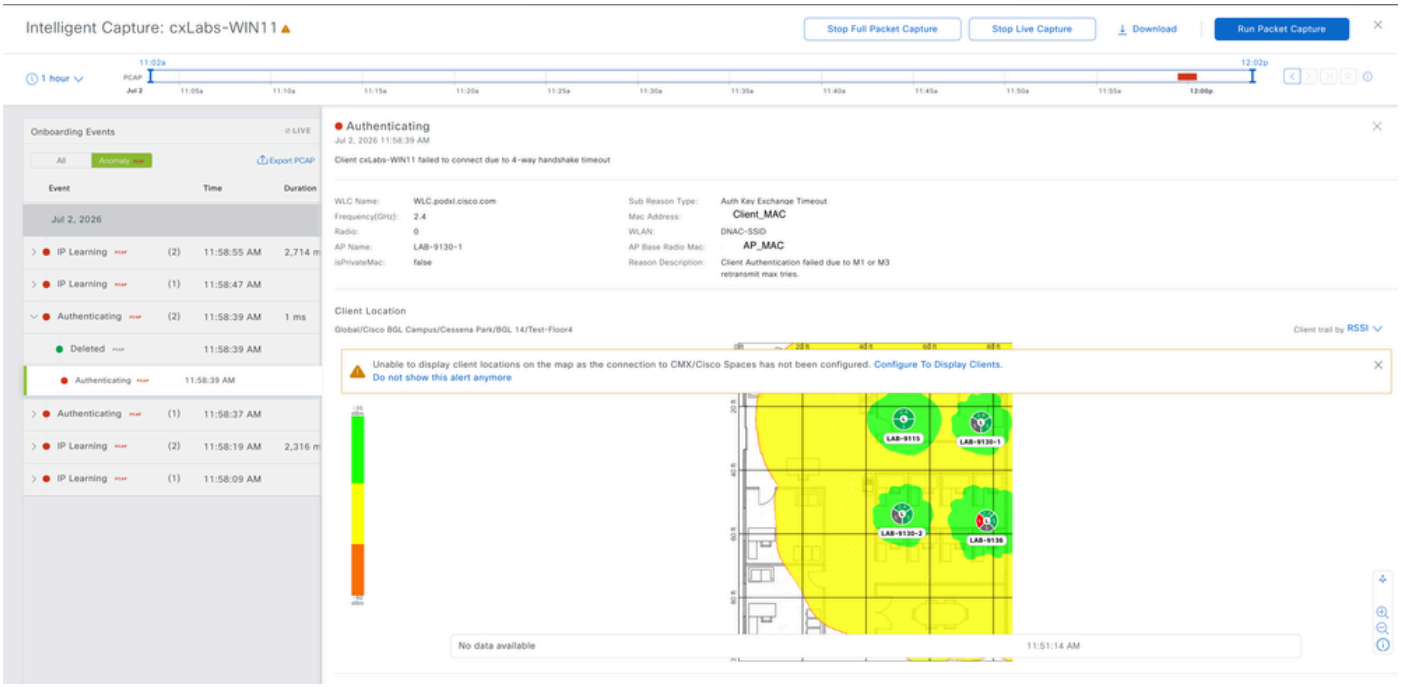


Aperçu de configuration pour capture d'anomalies

Une fois activé, il collecte en permanence les comportements d'anomalie pour les clients associés au point d'accès, et ceux-ci peuvent être visualisés dans les captures intelligentes (intégration et complète) prises pour des ID de client spécifiques.



Vue Anomaly Capture pour le client



Détails de capture d'anomalie pour le client

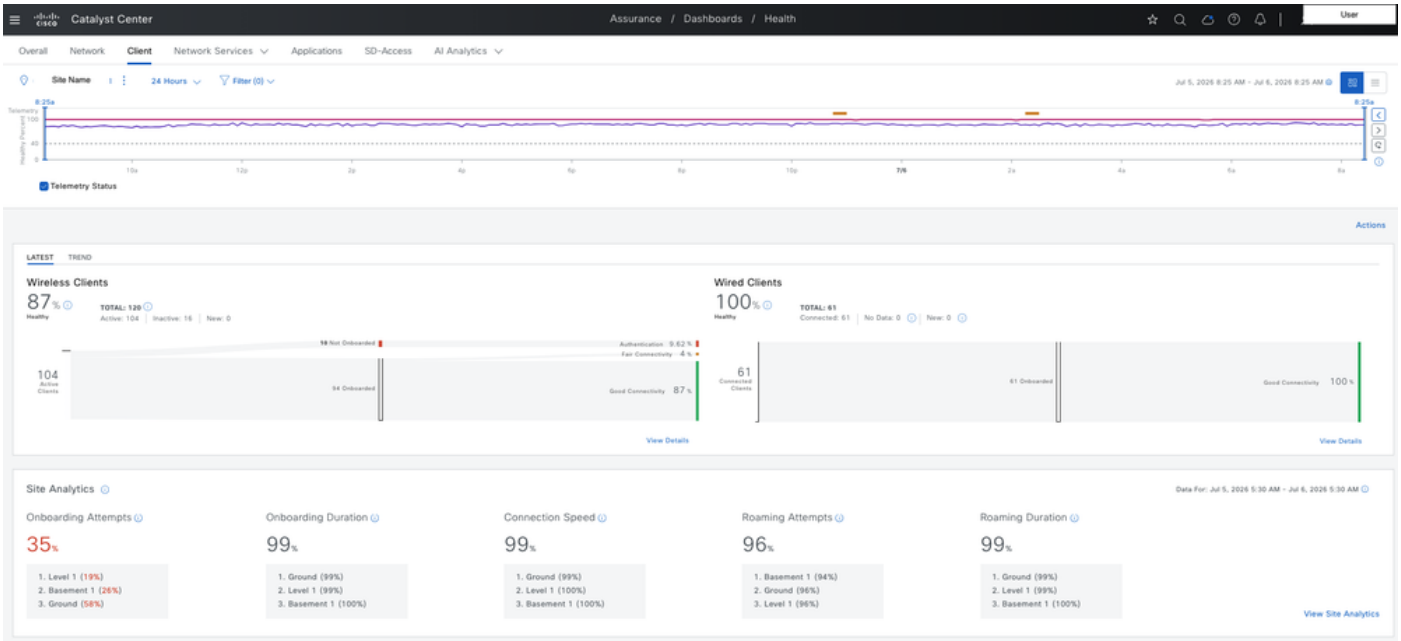
Cela nous permet de dépanner les comportements client irréguliers ou inattendus, tels que l'échec d'intégration, les problèmes d'authentification ou les modèles d'association anormaux, en détectant et en marquant automatiquement ces événements pour les points d'accès où il est activé. Associée à l'intégration et aux captures complètes de paquets pour des ID client spécifiques, elle permet aux administrateurs de suivre la séquence exacte des événements

conduisant à une anomalie, ce qui facilite l'identification des causes premières des problèmes récurrents de connectivité ou de performances des clients sans surveiller manuellement chaque session client.

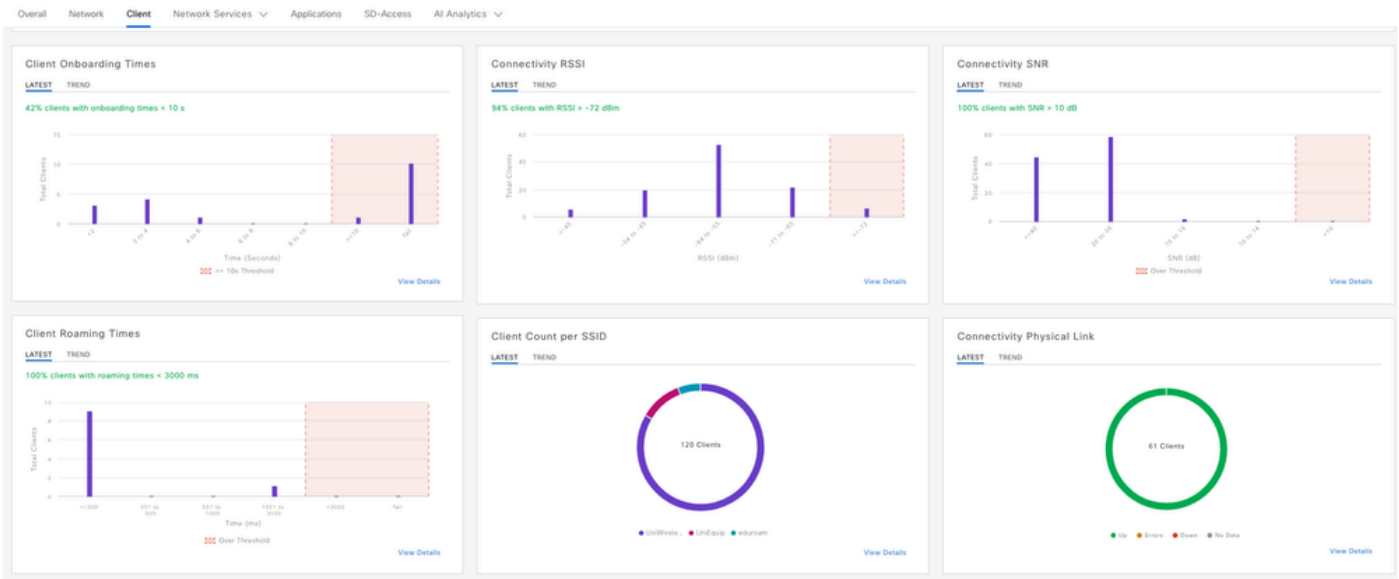
Problème de connectivité client sans fil

Les problèmes des clients sans fil (pannes d'intégration, interruptions d'itinérance, interférences RF ou connectivité intermittente) sont souvent transitoires et difficiles à reproduire. La surveillance traditionnelle basée sur des interrogations est donc insuffisante pour résoudre les problèmes. Cisco Catalyst Center résout ce problème grâce à une télémétrie continue de moins d'une seconde collectée directement à partir des points d'accès et des contrôleurs sans fil, corrélée entre les flux de travail Device 360, Client 360 et Intelligent Capture. Cette architecture basée sur la télémétrie permet de reconstruire les conditions RF et de niveau de protocole exactes au moment de la défaillance, de l'utilisation du canal et des interférences aux trames d'intégration 802.11.

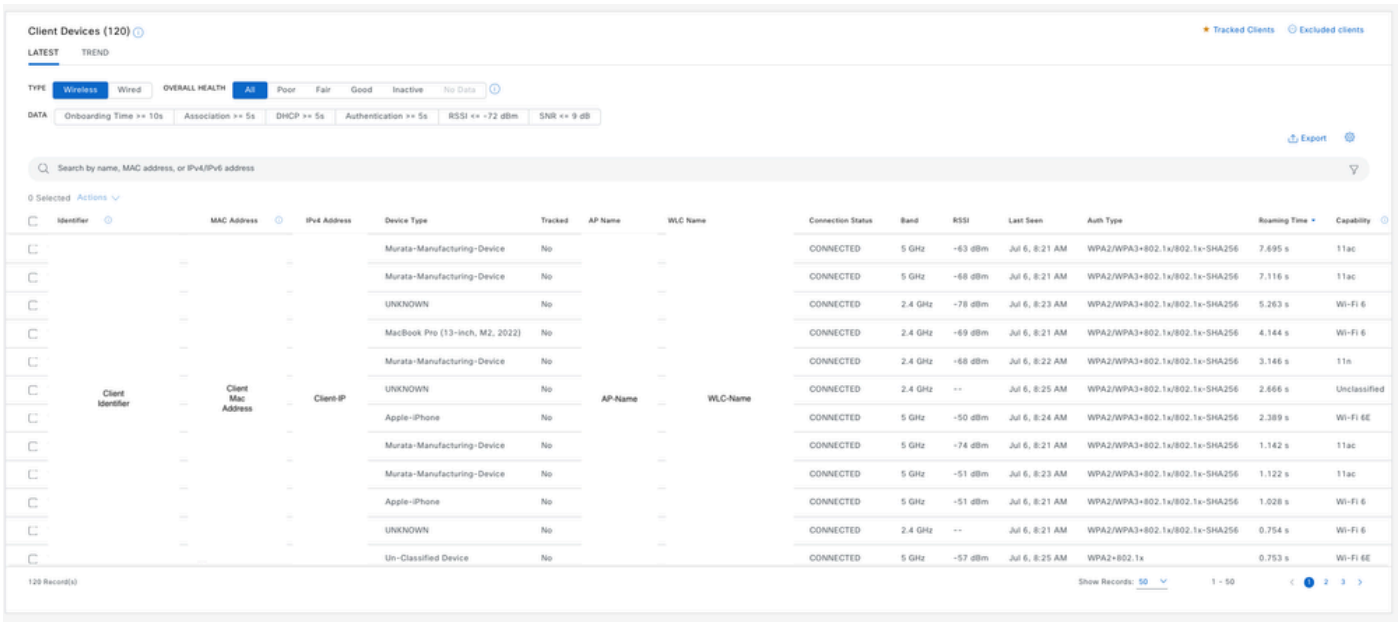
La section Client Health (Intégrité du client) fournit une vue d'ensemble complète des statistiques relatives aux clients sans fil sur tous les sites. Cela inclut des mesures clés telles que les performances d'intégration, RSSI, SNR, l'activité d'itinérance, la distribution par SSID et par radio, les débits de données et l'état de connectivité physique. Vous pouvez filtrer ces données en fonction d'un site spécifique et afficher les tendances historiques remontant aux 30 derniers jours, ce qui vous donne à la fois une perspective à l'échelle du réseau et une granularité au niveau du site. Accédez à Assurance > Dashboard > Health > Client.



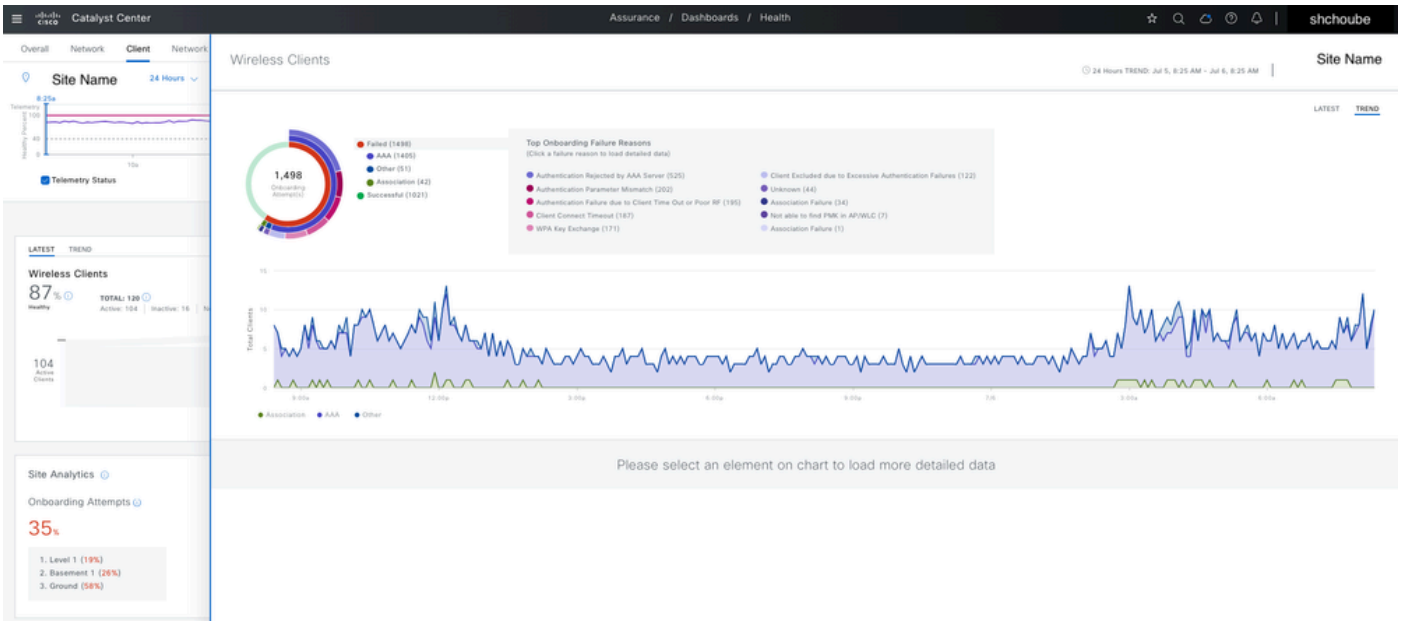
Statistiques client sans fil sur Catalyst Center



Statistiques client sans fil sur Catalyst Center

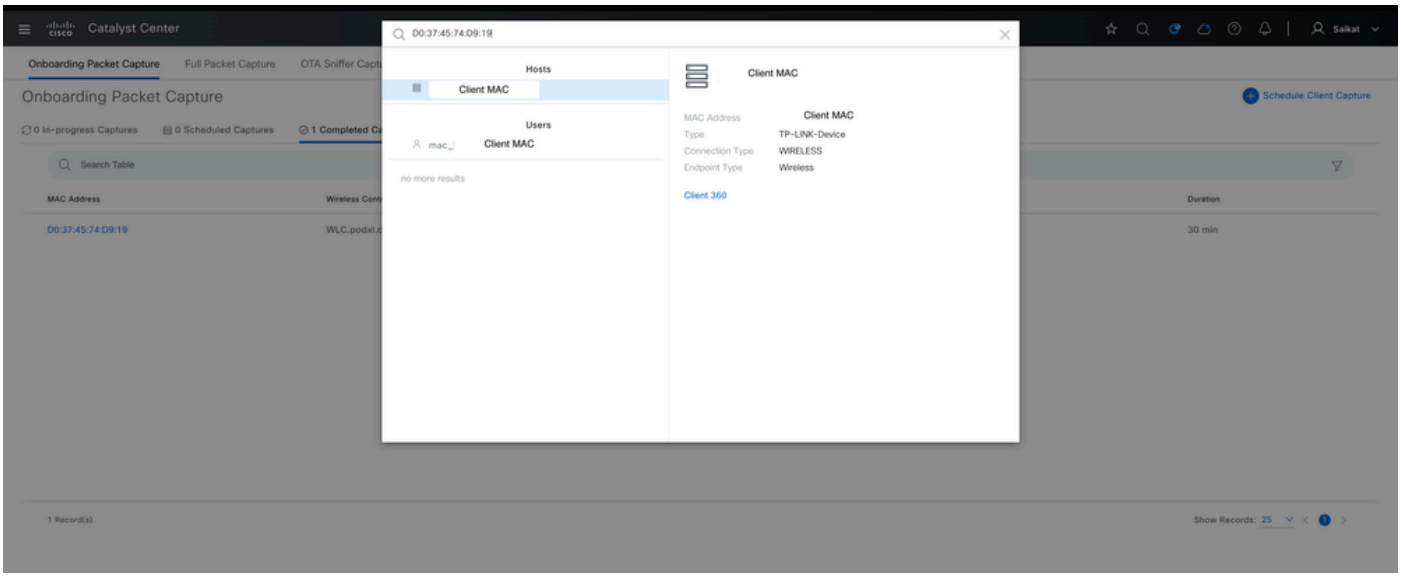


Statistiques client sans fil sur Catalyst Center

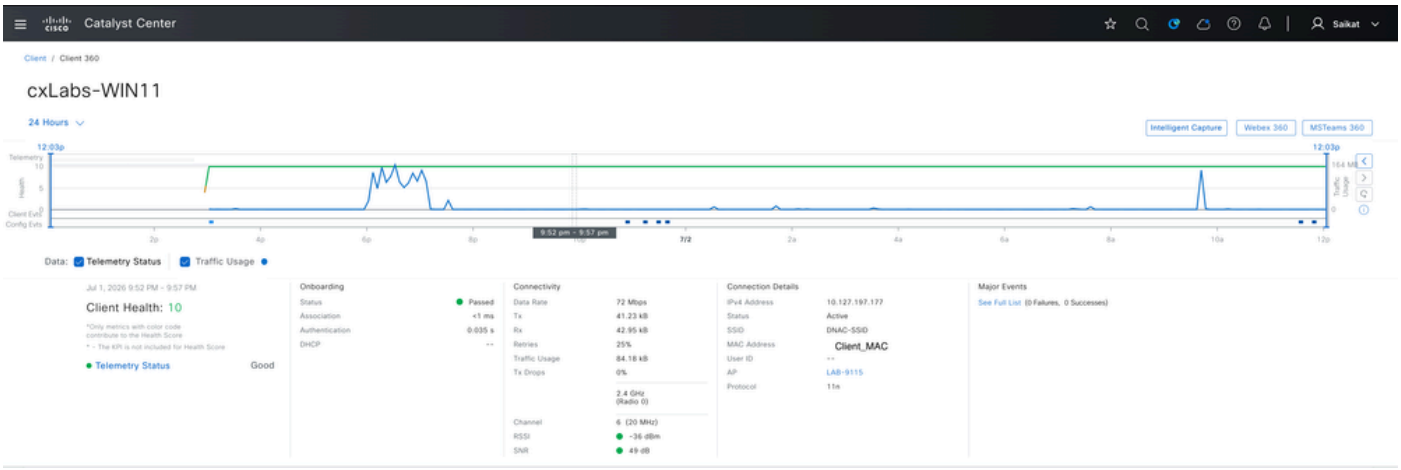


Statistiques client sans fil sur Catalyst Center

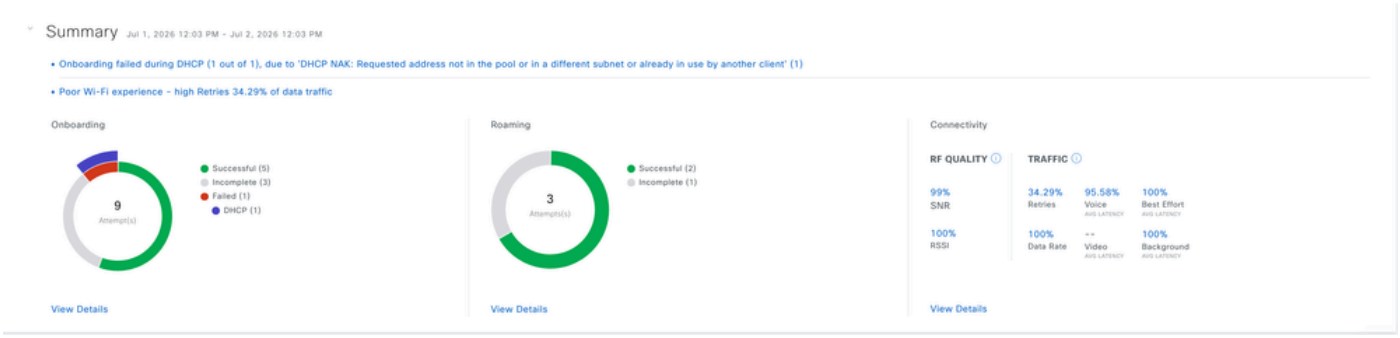
Pour le dépannage d'un client spécifique, vous pouvez effectuer une recherche à l'aide de l'adresse MAC du client, qui vous amène à la vue Client 360. Cette page présente des statistiques détaillées, spécifiques au client, notamment l'historique d'intégration, les événements de connectivité, les mesures RF et les détails de session. Ces statistiques s'appliquent exclusivement à ce client, ce qui permet une analyse précise de la cause première des problèmes rencontrés par chaque client.



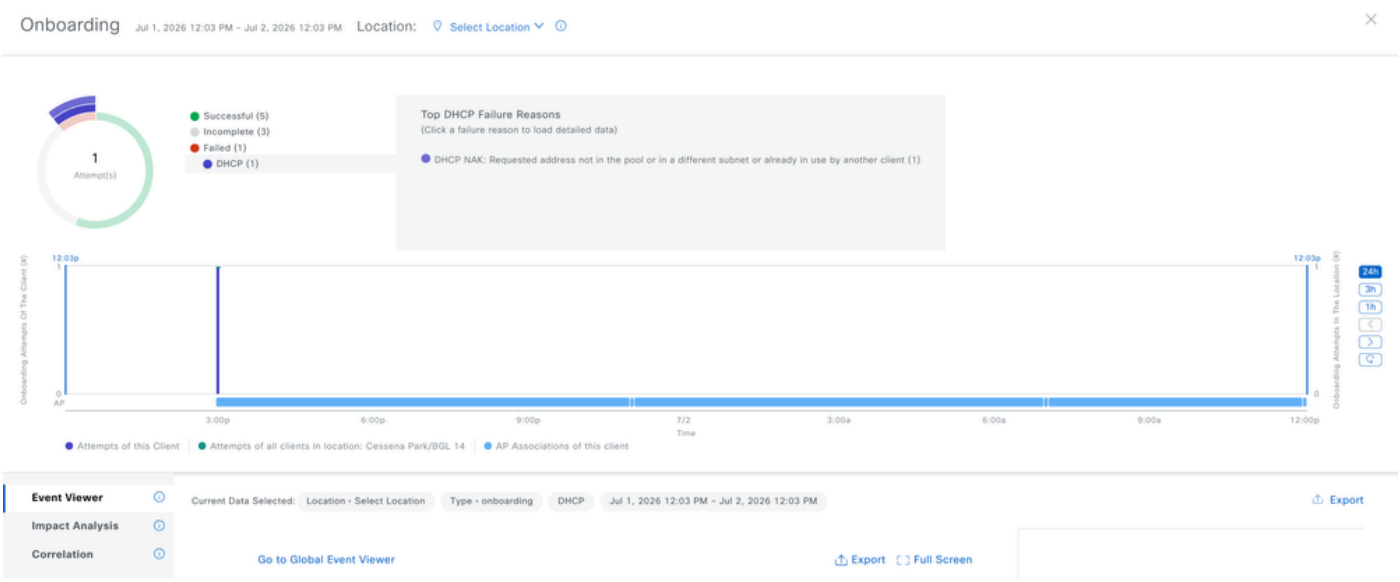
Périphérique d'adresse Mac client spécifique 360



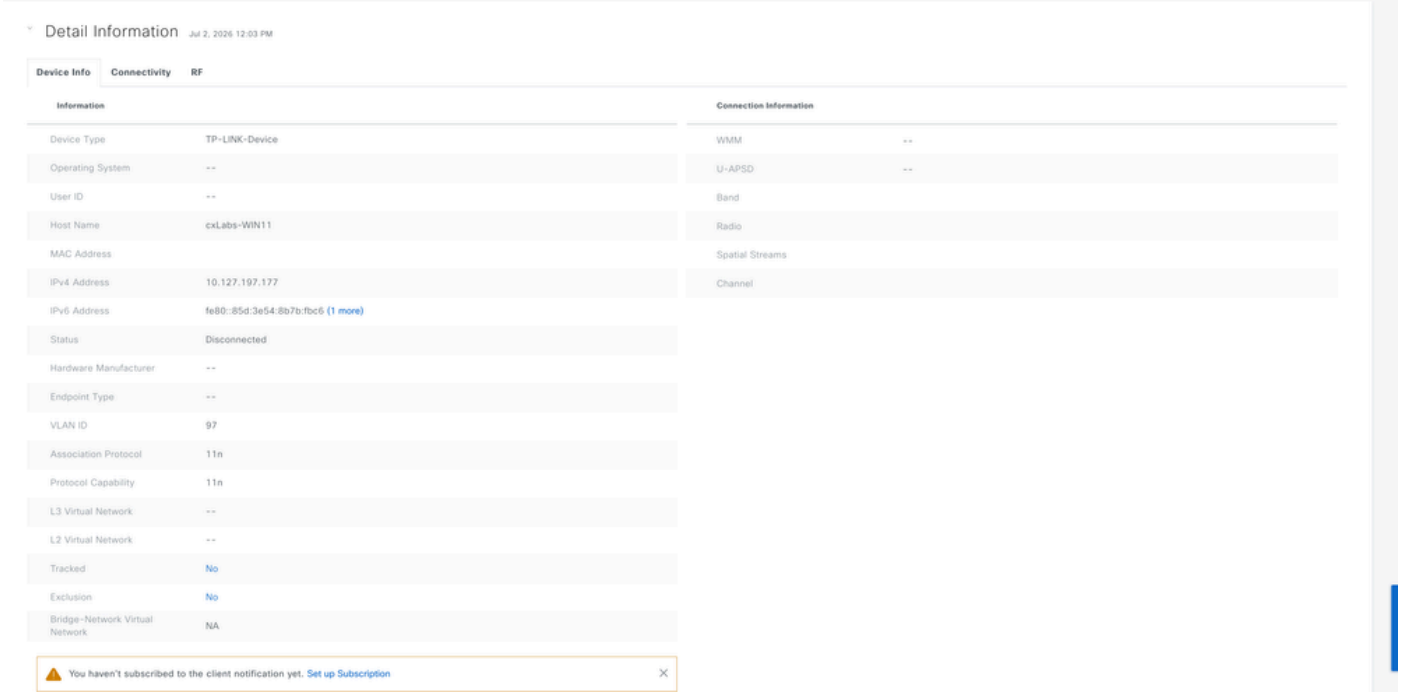
Télémétrie + état de santé du client



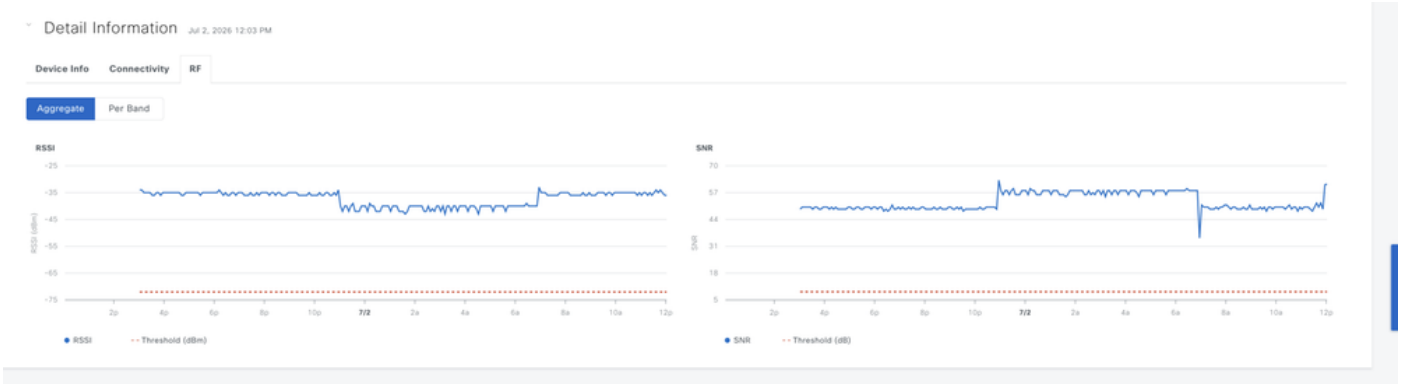
Résumé global pour le client



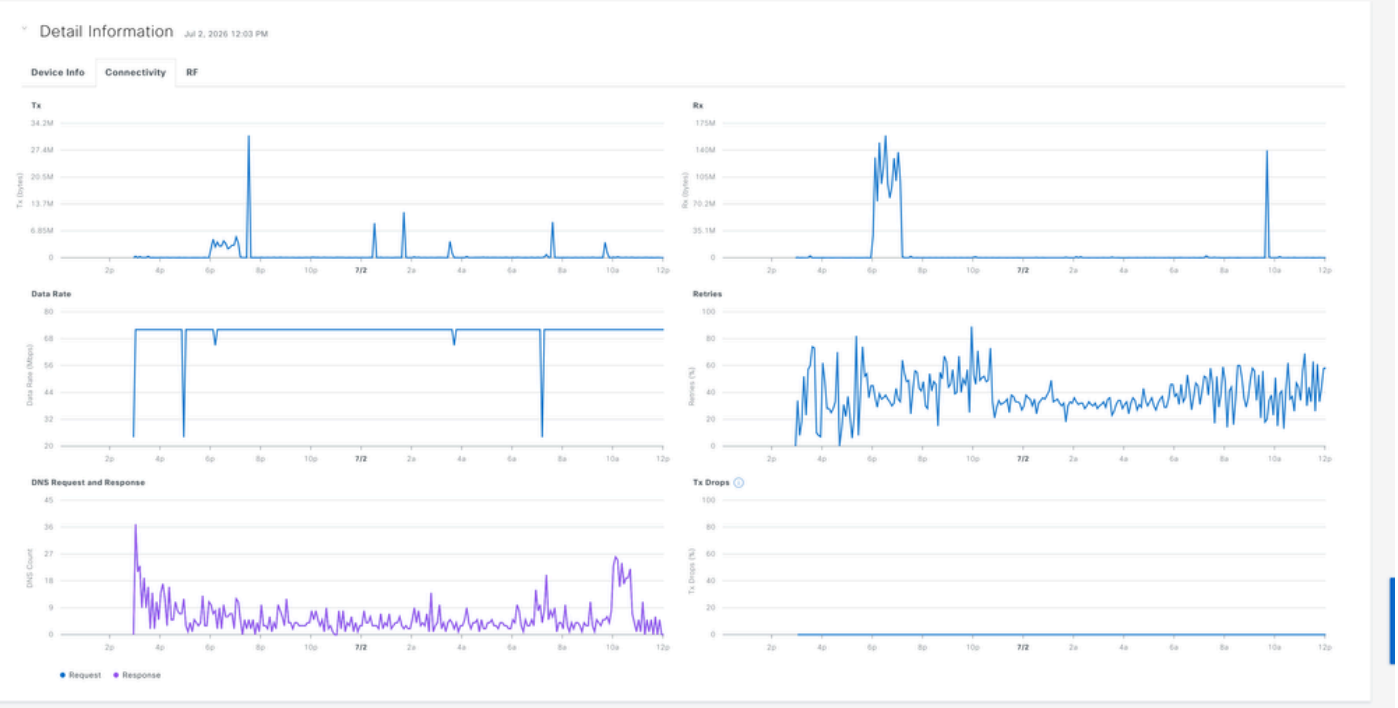
Événement signalé pour le client en détail



Détails du périphérique client



Statistiques RF pour le client



Statistiques de connectivité pour le client

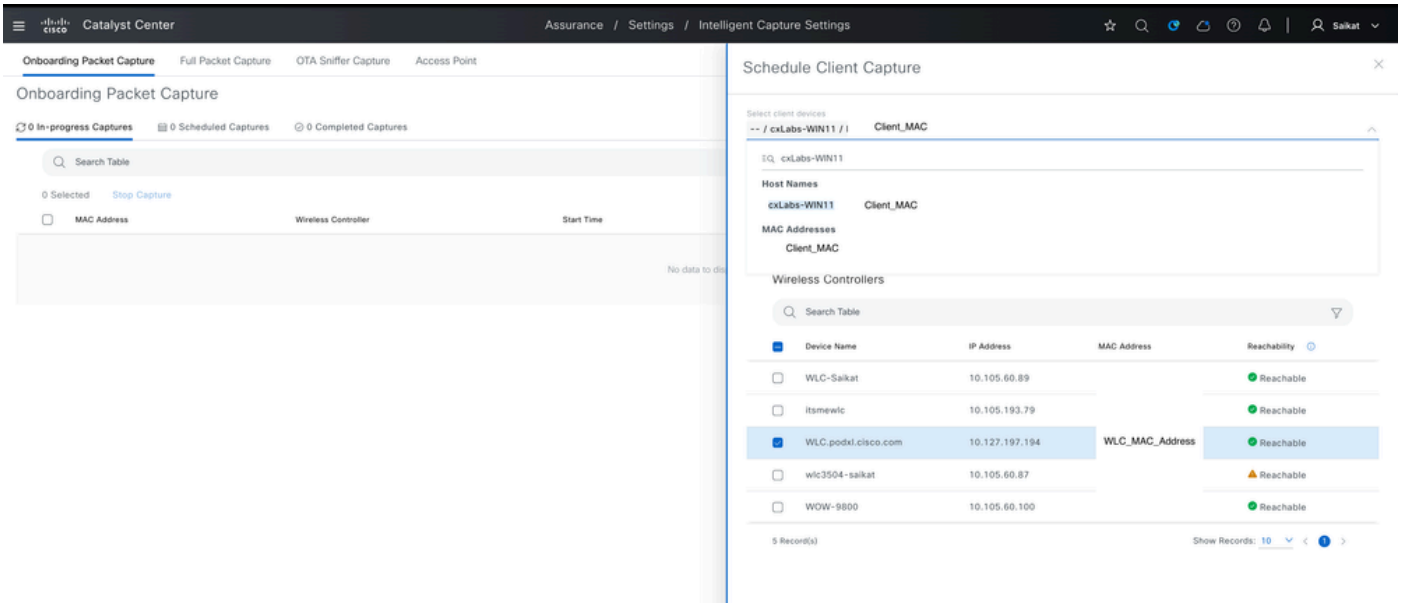
Captures intelligentes pour les clients sans fil

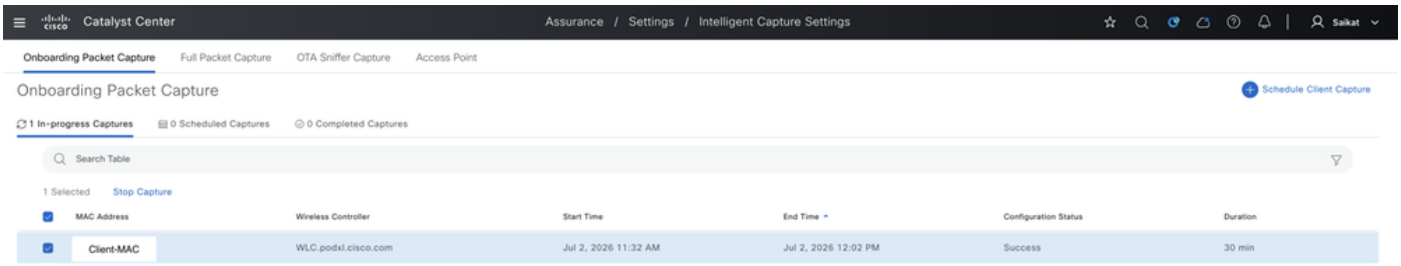
La capture intelligente (iCAP) aide à résoudre les problèmes de connectivité des clients sans fil en capturant des données réelles au niveau des paquets directement à partir de Catalyst Center. Il peut capturer les trames de gestion 802.11, DHCP et EAP pour identifier l'échec d'une tentative de connexion, les données non chiffrées et les paquets de gestion pour un client spécifique afin de résoudre les problèmes d'intégration, d'accessibilité et d'application. Vous pouvez également programmer des captures intelligentes pour une exécution ultérieure, en fonction des besoins. La durée par défaut de la session est de 30 minutes et peut être définie sur huit heures.

Intégration de la capture de paquets

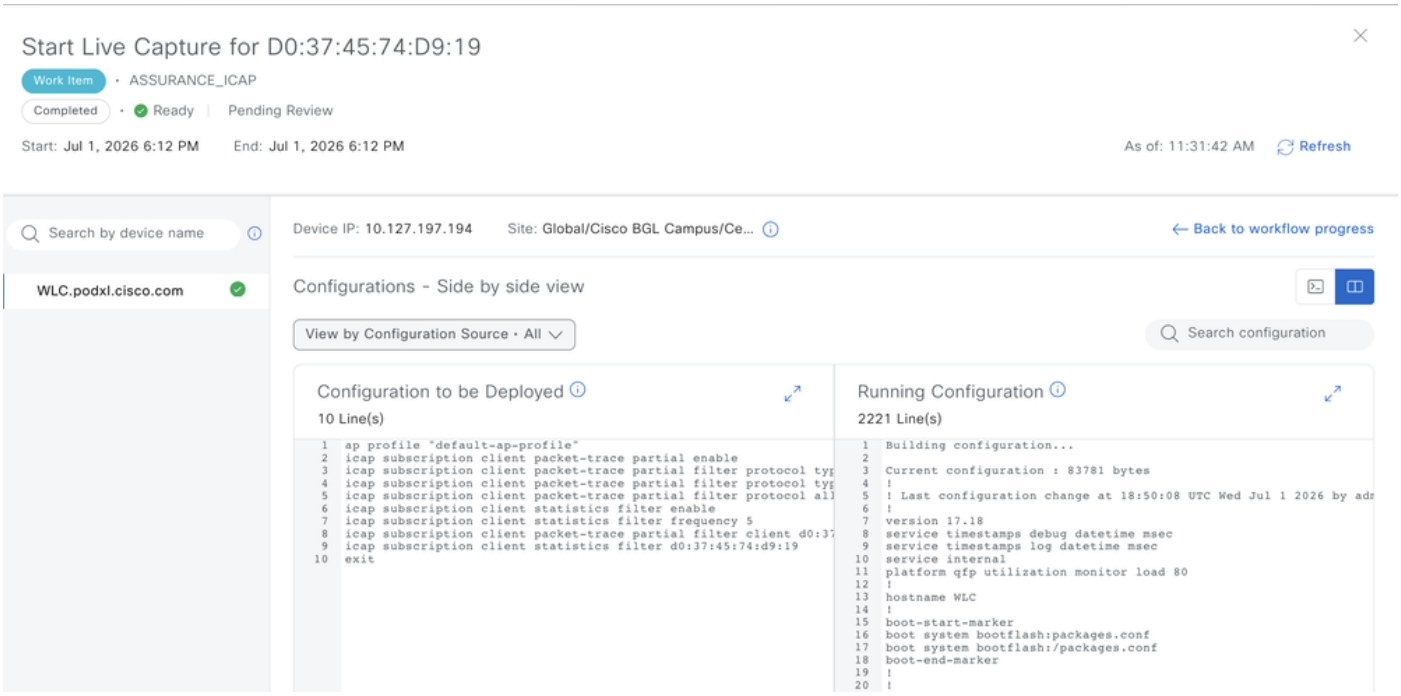
L'intégration de la capture de paquets enregistre la séquence de paquets qu'un périphérique client échange lorsqu'il tente de se connecter au réseau sans fil, y compris les trames de gestion 802.11 (telles que les demandes d'association et d'authentification), les paquets DHCP et les paquets EAP utilisés lors de l'authentification 802.1X. Parallèlement, il collecte les statistiques RF des clients, ce qui permet de visualiser les conditions du signal au moment exact de l'intégration. Ces captures sont utiles pour le dépannage d’un scénario dans lequel un client ne parvient pas à se connecter et aident à déterminer l’étape précise (lors de l’association, de l’authentification ou de l’attribution d’adresses IP) à laquelle se produit l’échec. Par défaut, la capture de paquets d'intégration est activée sur le dernier contrôleur sans fil connecté au client. Sélectionnez jusqu'à trois contrôleurs sans fil pour couvrir le scénario d'itinérance client.

Pour activer la capture de paquets d'intégration, accédez à Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Schedule Client Capture (en haut à droite) > search for Client Identifier (adresse Mac).



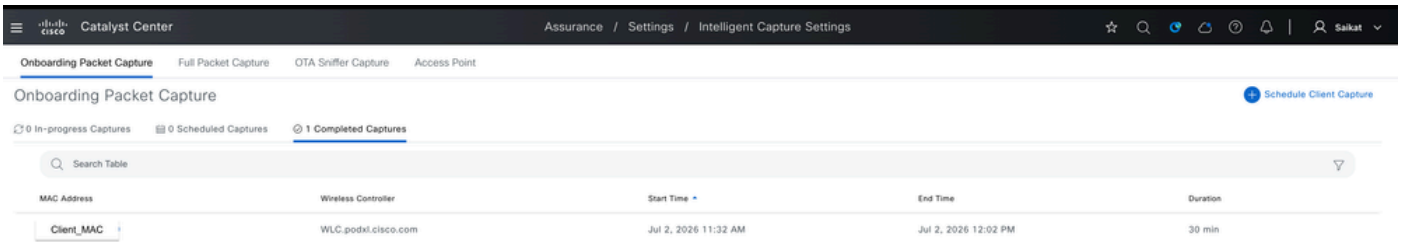


Capture d'intégration planifiée

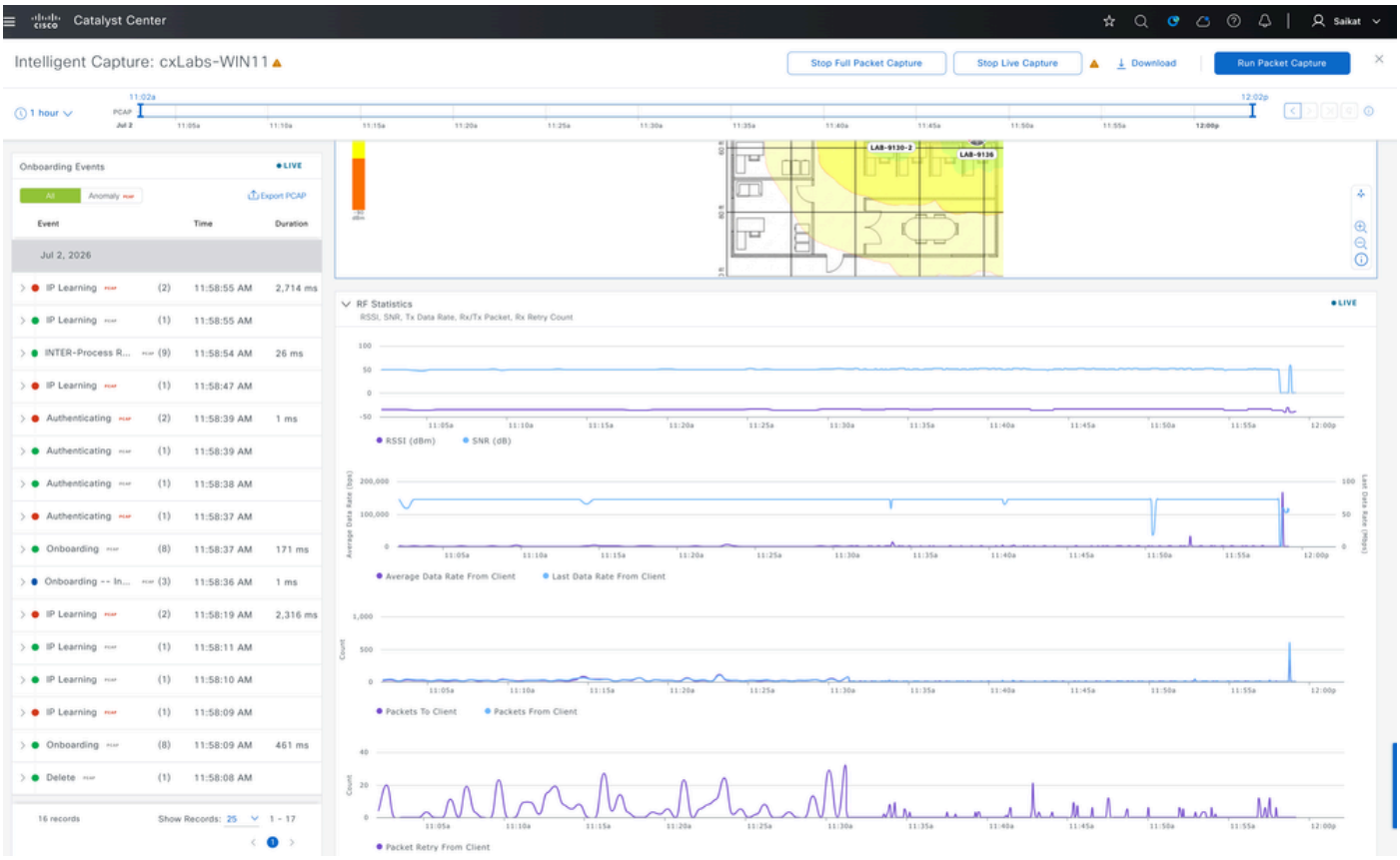


Aperçu de la configuration pour la capture d'intégration

La capture d'intégration peut être arrêtée manuellement ou automatiquement désactivée une fois la durée planifiée (comprise entre 30 minutes et 8 heures) écoulée. Une fois arrêtée, la capture apparaît sous Captures terminées, où vous pouvez cliquer sur l'adresse MAC du client pour afficher les données de capture détaillées et exporter le fichier au format PCAP pour une analyse plus approfondie.



Capture d'intégration terminée

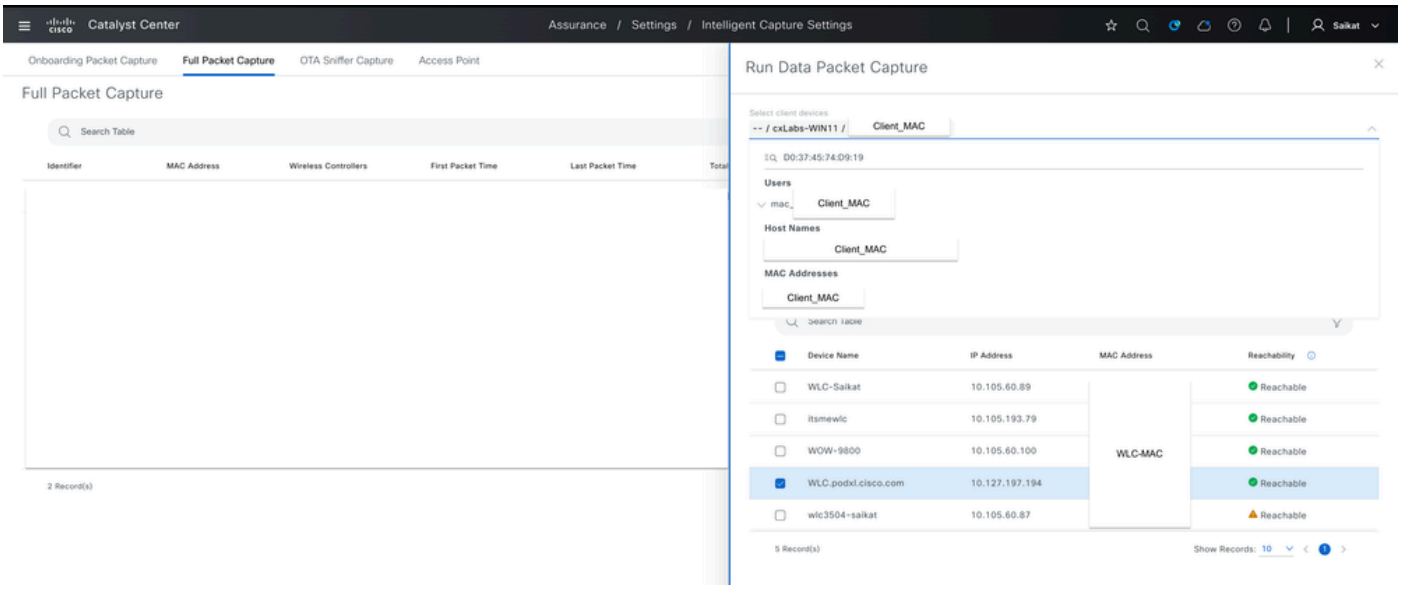


Exemple de capture d'intégration complète

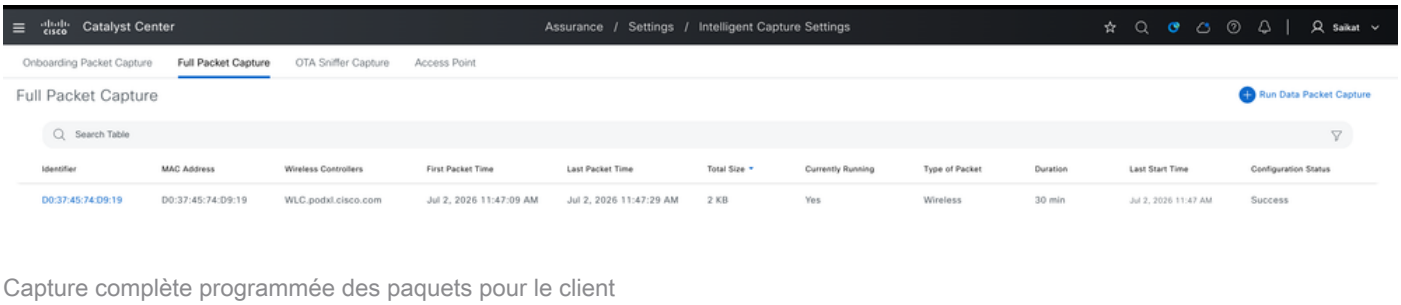
Capture de paquets complète

Une session de capture de paquets complète peut capturer des données complètes pour un client spécifique, fournissant une visibilité approfondie au niveau des paquets sur le trafic sans fil continu de ce client, ce qui nous permet d'inspecter les paquets de données et de gestion en détail pour dépanner les problèmes d'accès, les problèmes de performances des applications ou d'autres anomalies de connectivité qui vont au-delà de ce que les statistiques RF standard peuvent révéler. Il peut capturer jusqu'à 1 Go de données évolutives pour un client spécifique et conserve en permanence les données les plus récentes jusqu'à la limite.

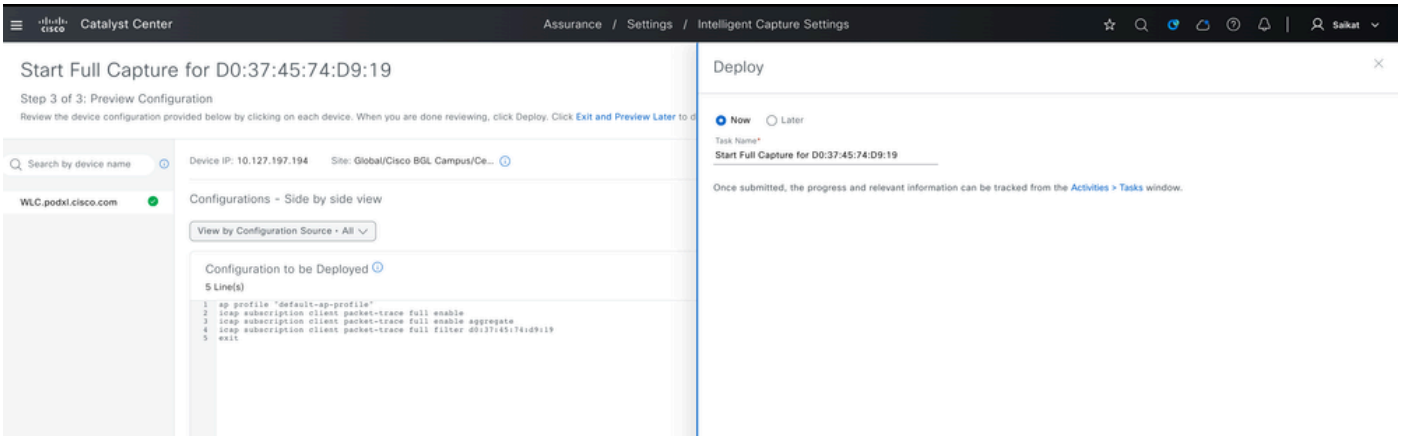
Pour activer la capture complète des paquets, accédez à Assurance > Settings > Intelligent Capture Settings > Onboarding Capture > Run Data Capture (en haut à droite) > Search for Client Identifier (adresse Mac) :



Capture complète des paquets pour le client



Capture complète programmée des paquets pour le client



Aperçu de la configuration pour la capture complète des paquets

La capture complète des paquets peut être arrêtée manuellement ou automatiquement désactivée une fois la durée planifiée (comprise entre 30 minutes et 8 heures) écoulée. Une fois arrêtée, la capture apparaît sous Captures terminées, où vous pouvez cliquer sur l'adresse MAC du client pour afficher les données de capture détaillées et exporter le fichier au format PCAP pour une analyse plus approfondie.

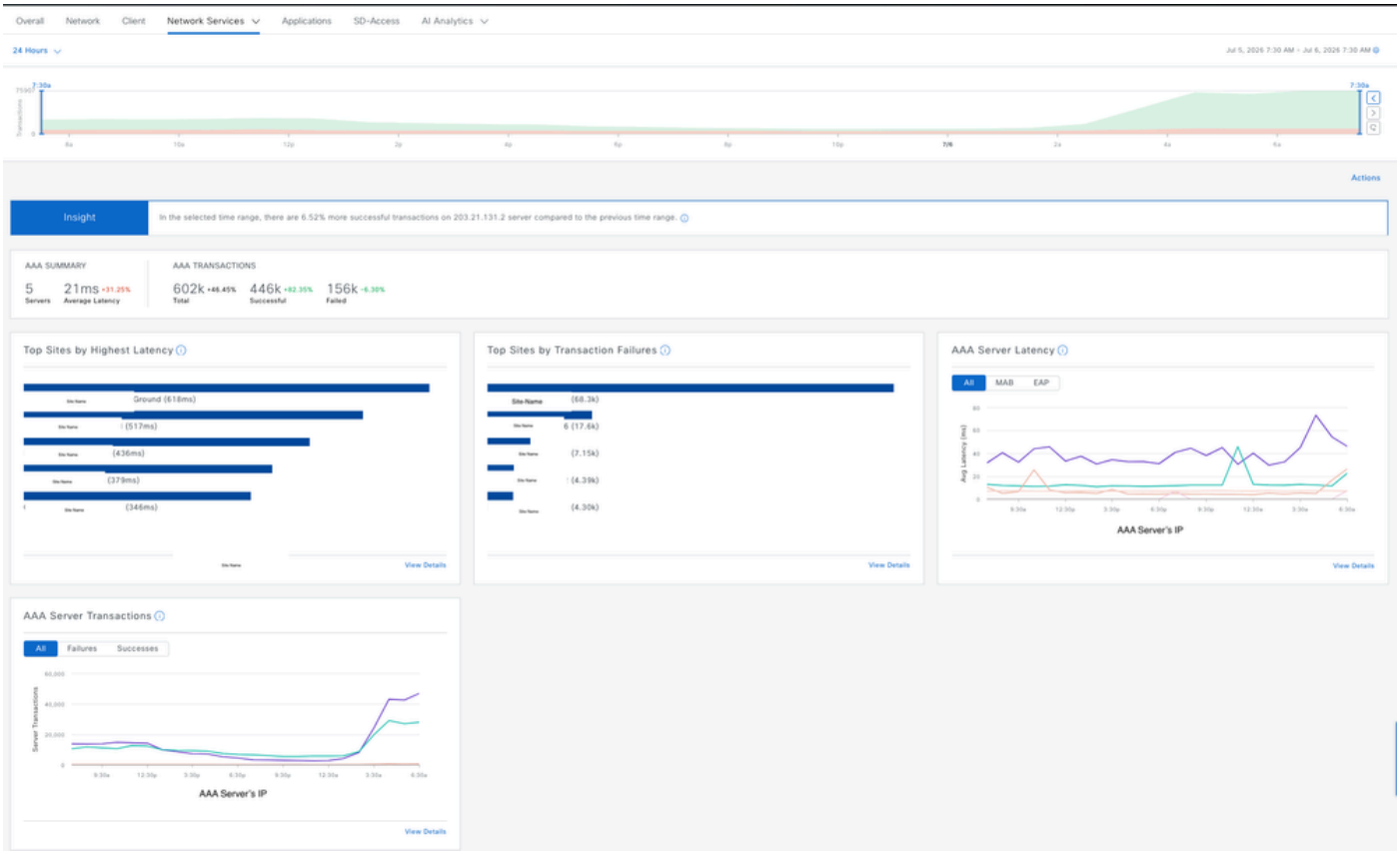


Exemple de capture complète collectée pour le client

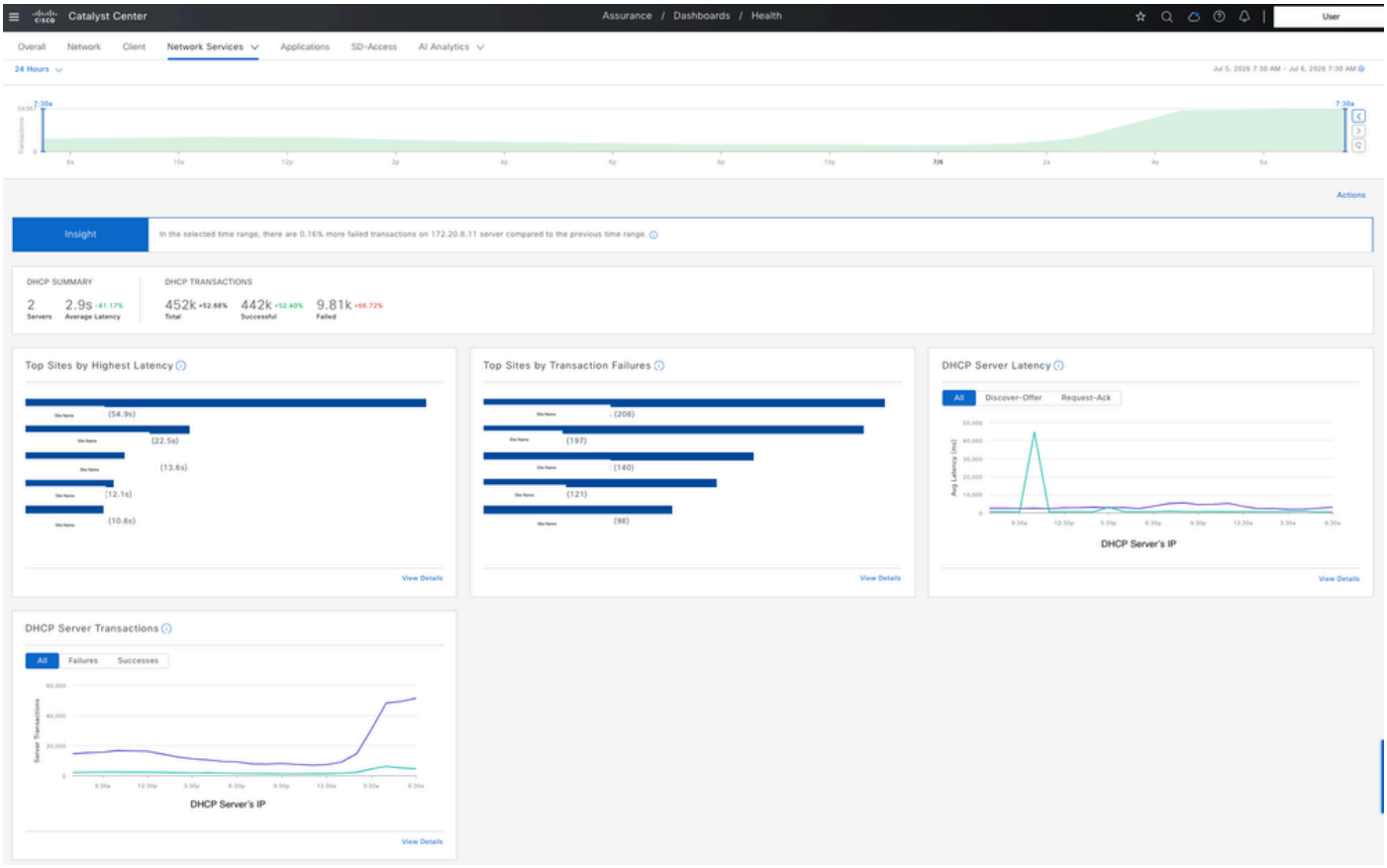
Isoler les problèmes de service réseau (AAA, DHCP, DNS)

Si le symptôme signalé pointe vers un service réseau spécifique plutôt que vers le contrôleur lui-même (par exemple, des clients ne parvenant pas à s'authentifier, ne recevant pas d'adresse IP ou ne parvenant pas à résoudre un nom), le tableau de bord des services réseau Catalyst Center sous Assurance vous donne une visibilité sur ces transactions telles qu'elles sont signalées par le WLC.

Accédez à Assurance > Dashboard > Health > Network services > AAA/DHCP/DNS :



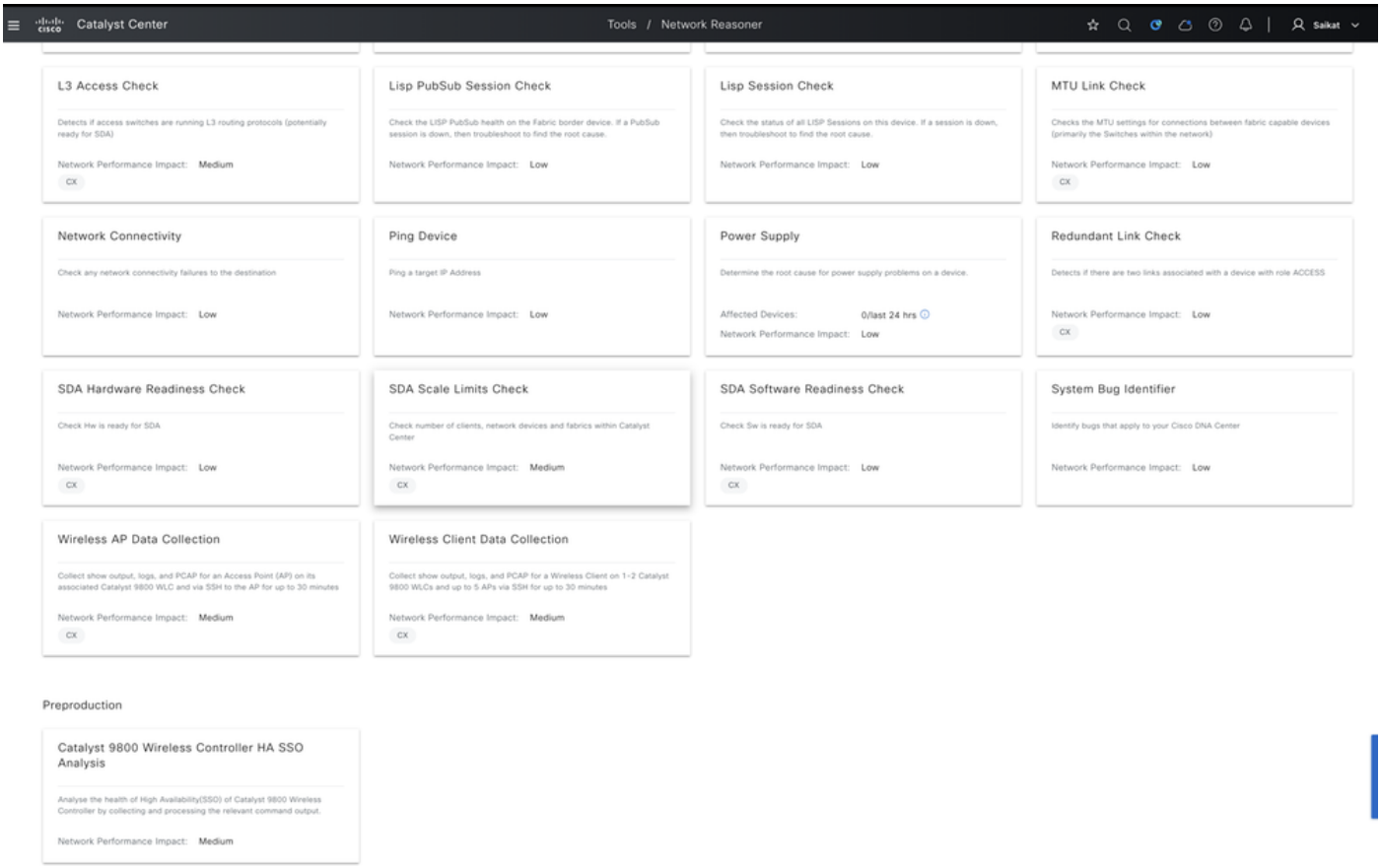
Statistiques AAA du client sans fil sur Catalyst Center



Statistiques DHCP du client sans fil sur Catalyst Center

Raisonneur de réseau

Network Reasoner est un outil intégré de Catalyst Center qui analyse automatiquement les problèmes réseau à votre place. Vous n'avez pas besoin de parcourir les journaux manuellement. Vous pouvez le trouver sous Outils > Raisonneur de réseau. Chaque option de dépannage (appelée workflow) affiche une brève description, le nombre de périphériques affectés au cours des dernières 24 heures et ce qui se passe si vous l'exécutez. Il ne peut détecter que les problèmes sur les périphériques qui sont soit ajoutés à Catalyst Center pour la surveillance Assurance, soit provisionnés via Catalyst Center.



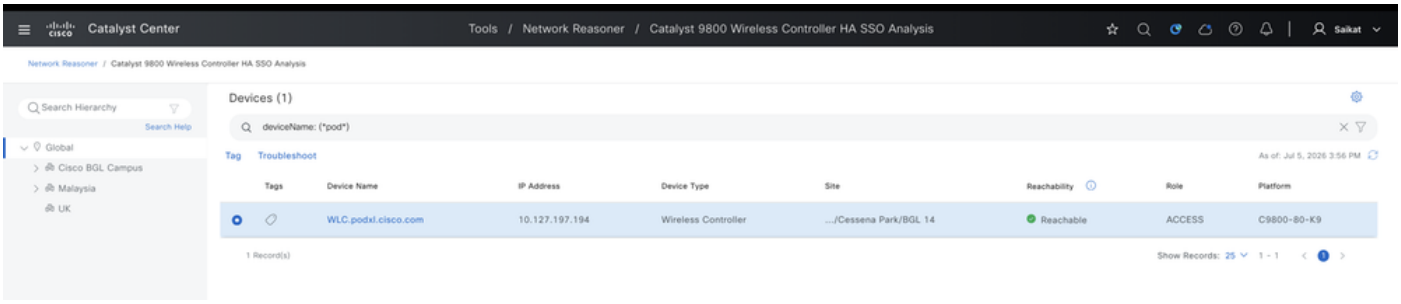
Diverses options de dépannage réseau disponibles sur Network Reasoner

Pour les réseaux sans fil, vous pouvez résoudre trois problèmes principaux :

1. Pour les problèmes de contrôleur, en particulier avec les configurations haute disponibilité, Network Reasoner vérifie les éléments suivants :

- Le contrôleur est-il accessible ?
- La haute disponibilité est-elle correctement configurée ?
- Les contrôleurs actif et en veille sont-ils synchronisés ?
- La connexion entre eux fonctionne-t-elle ?

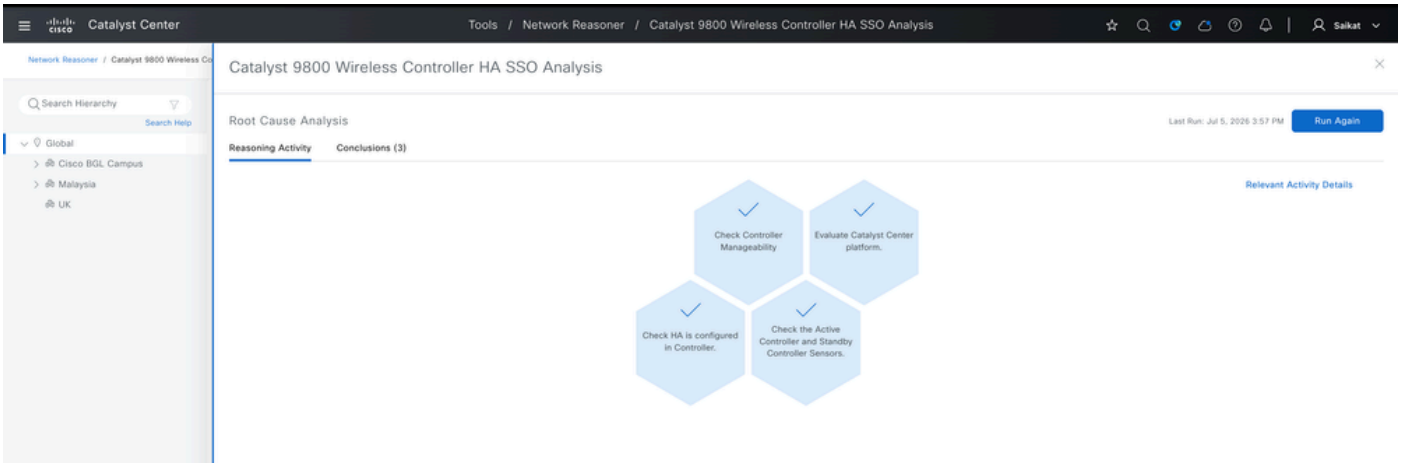
S'il détecte un problème, il vous indique exactement ce qui ne va pas et vous suggère comment le résoudre. Il existe également une option distincte pour le dépannage des périphériques qui n'envoient aucune donnée de surveillance.



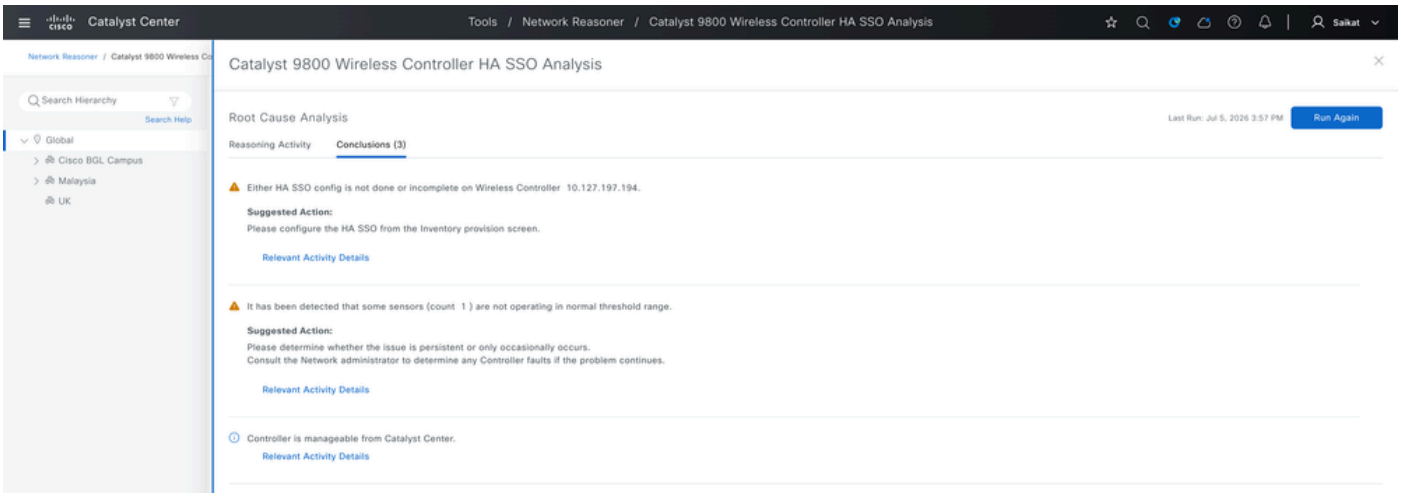
Dépannage de la haute disponibilité avec Network Reasoner

Lorsque vous activez la fonctionnalité de dépannage pour l'analyse HA SSO sur le WLC 9800 à l'aide de Network Reasoner, elle effectue plusieurs vérifications et fournit une conclusion basée sur les résultats. Si des problèmes sont détectés avec HA SSO, il suggère également des mesures correctives pour les résoudre.

```
!! Task Workflow !!
Check Controller Manageability
Evaluate Catalyst Center platform.
Check HA is configured in Controller.
Check the Active Controller and Standby Controller Sensors.
```

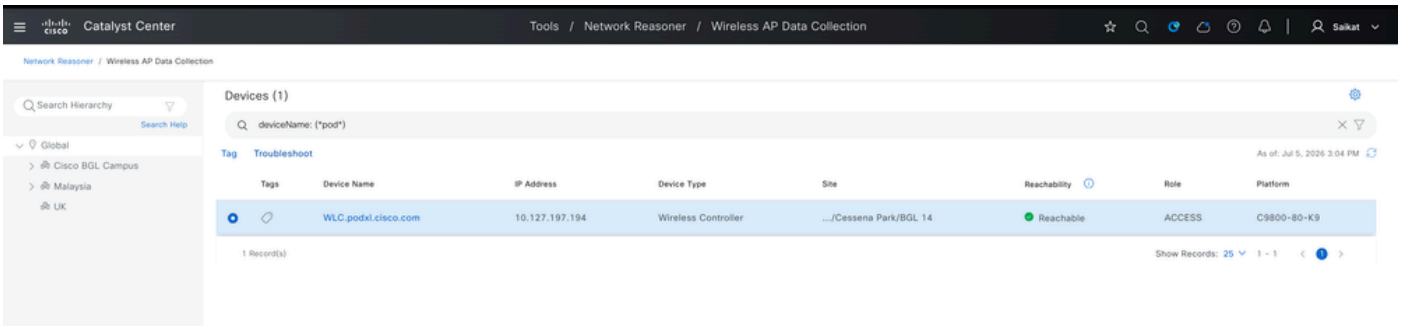


Tâches effectuées par CATC pour l'analyse SSO HA

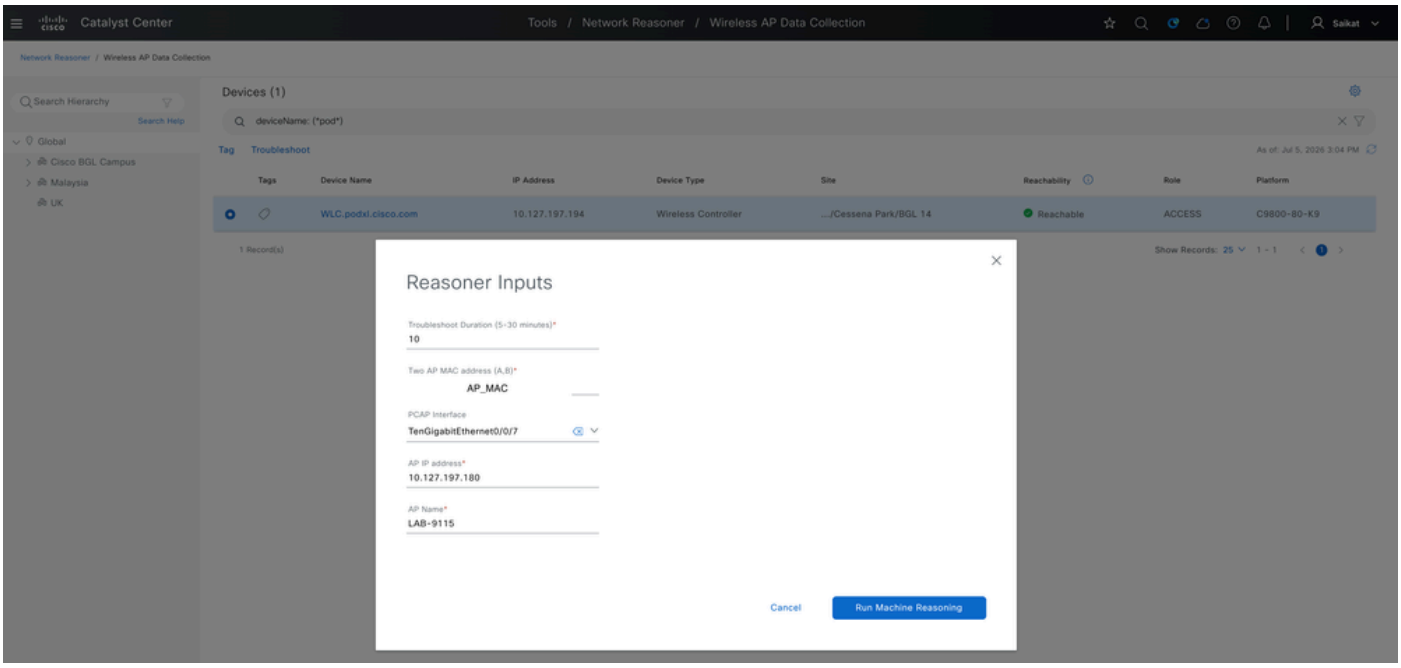


Exemple de conclusion pour le dépannage HA SSO à l'aide de Network Reasoner

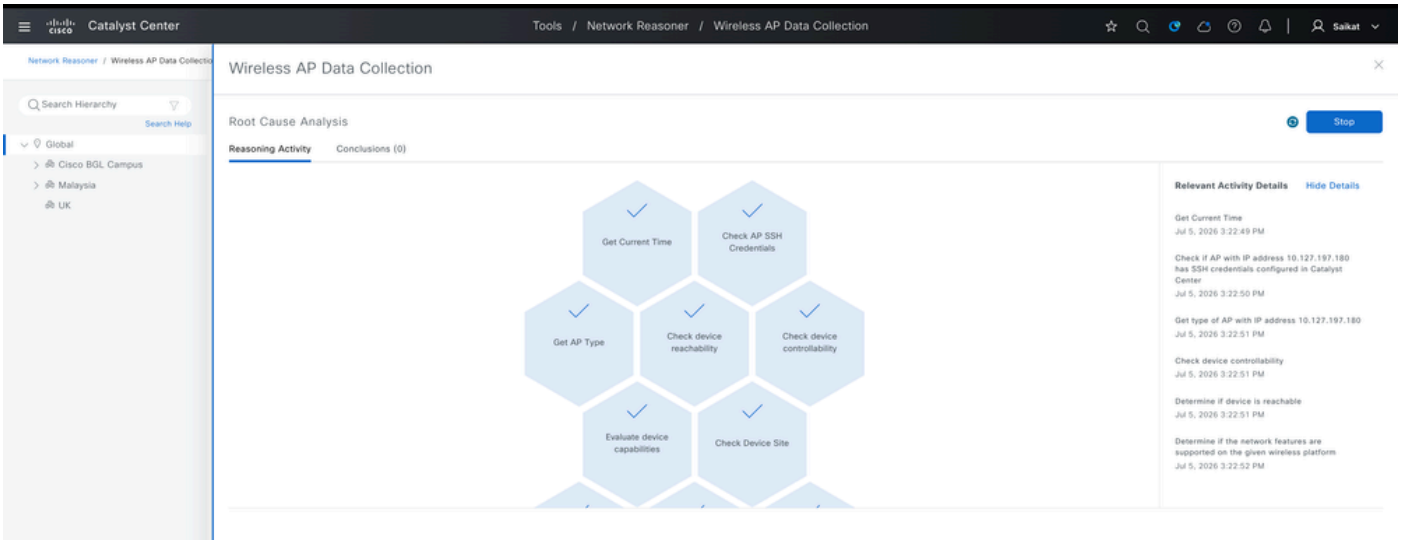
2. Points d'accès : si un point d'accès rencontre des problèmes, sélectionnez le contrôleur qui le gère, puis entrez l'adresse MAC des points d'accès et définissez la durée d'exécution de la vérification. Il permet la capture des journaux et des paquets depuis le WLC et le point d'accès, pour une visibilité plus approfondie. Voici le workflow d'activation de Network Reasoner pour un point d'accès, ainsi que les résultats correspondants :



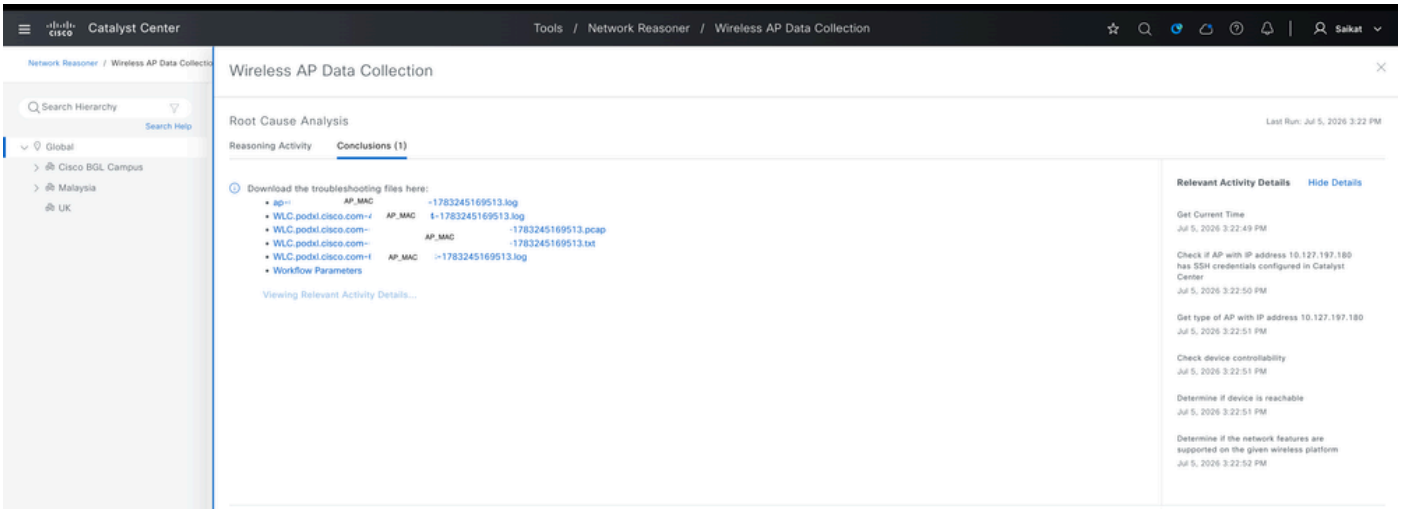
Sélectionnez Managed AP AP WLC pour dépanner



Fournir les détails du point d'accès pour dépanner



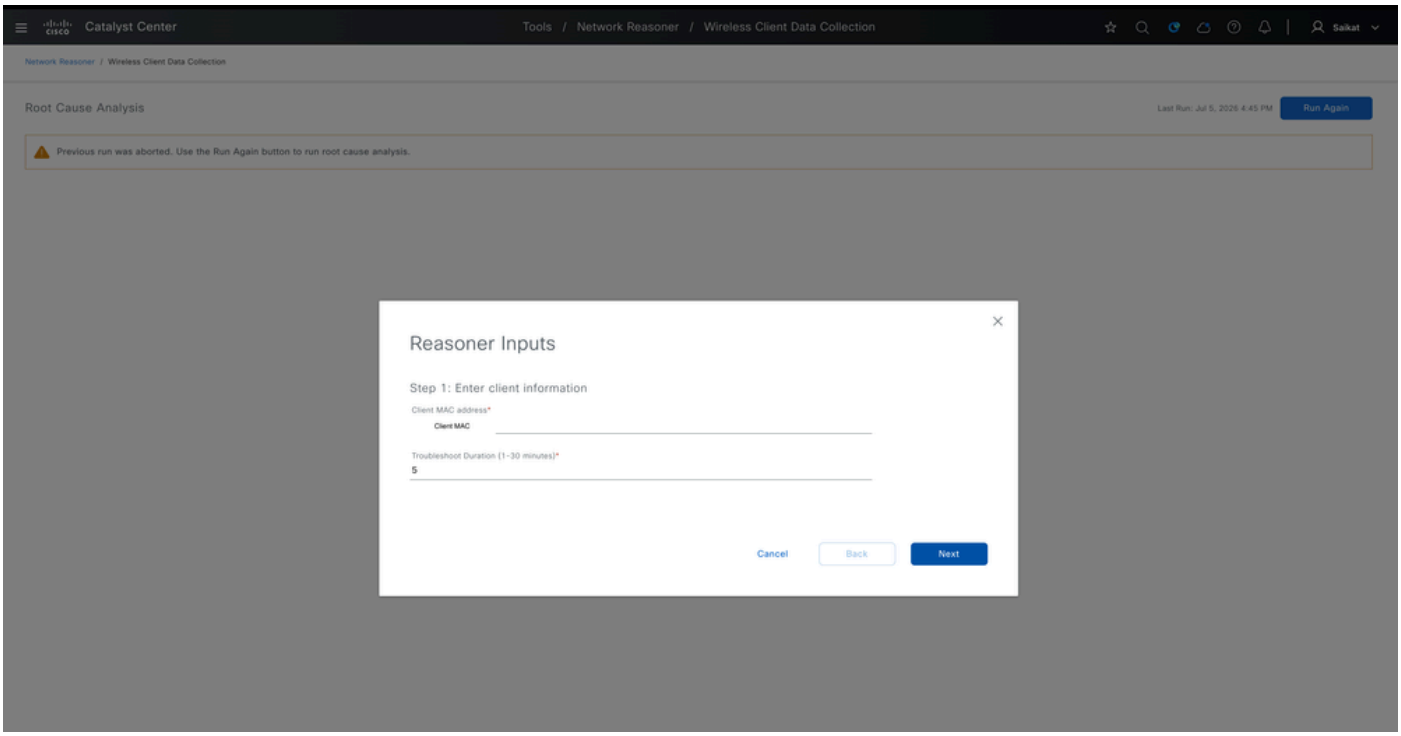
Tâches en cours pour dépanner un problème AP



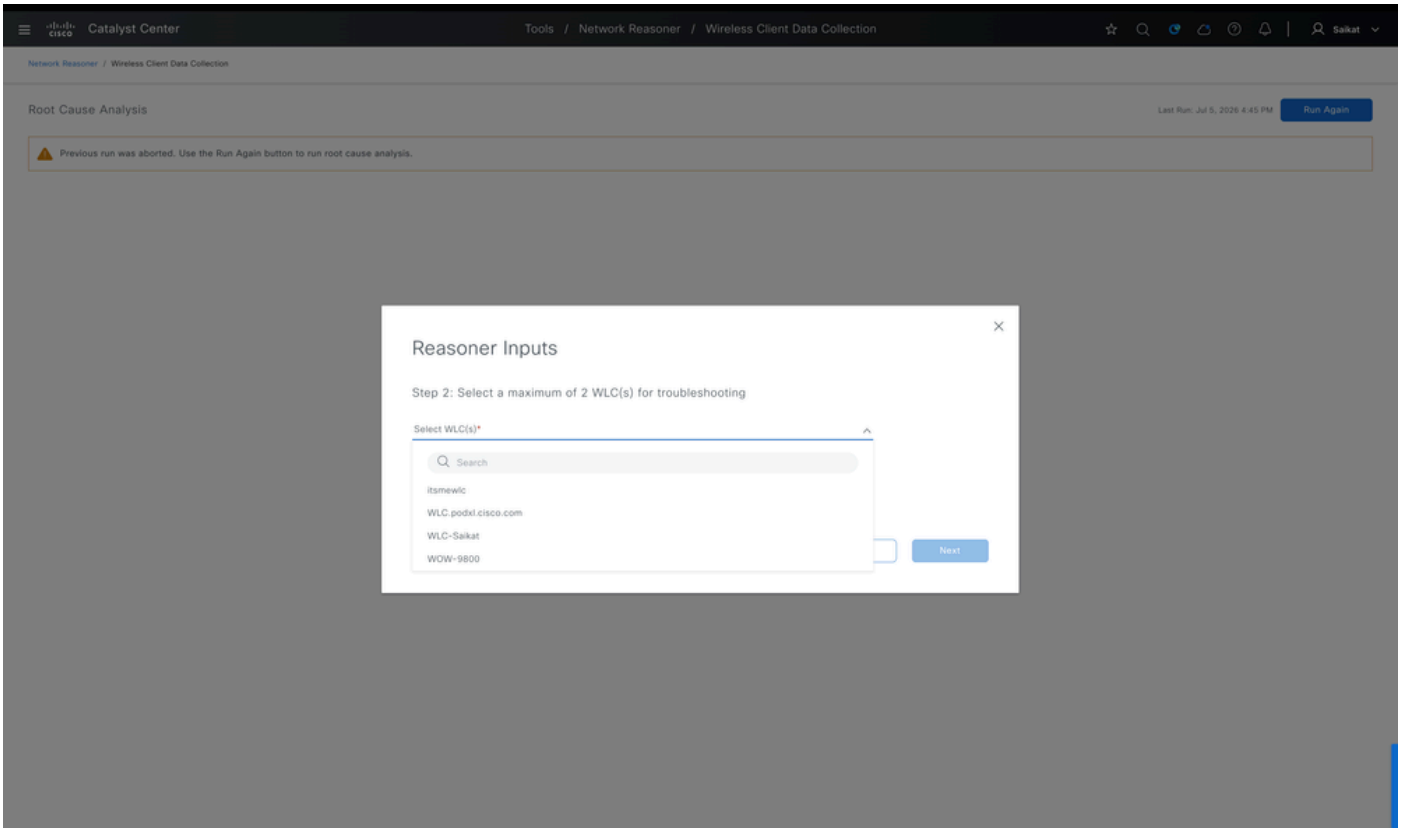
```
!! Task Workflow !!
Get Current Time
Jul 5, 2026 5:04:39 PM
Check if AP with IP address 10.127.197.180 has SSH credentials configured in Catalyst Center
Jul 5, 2026 5:04:40 PM
Get type of AP with IP address 10.127.197.180
Jul 5, 2026 5:04:40 PM
Check device controllability
Jul 5, 2026 5:04:41 PM
Determine if device is reachable
Jul 5, 2026 5:04:41 PM
Determine if the network features are supported on the given wireless platform
Jul 5, 2026 5:04:41 PM
Check if the device <device> is provisioned or assigned to a site.
Jul 5, 2026 5:04:42 PM
Start RA Trace
Jul 5, 2026 5:04:49 PM
Get Current Time
Jul 5, 2026 5:04:54 PM
Starting AP PCAP session <file-name> with filter 10.127.197.180 on interface TenGigabitEthernet0/0/7
Jul 5, 2026 5:04:55 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
Jul 5, 2026 5:04:57 PM
Start AP statistics collection on WLC with IP address 10.127.197.194 and wait for data collection for 3
Jul 5, 2026 5:04:58 PM
Start logging on COS AP with IP address 10.127.197.180 over SSH for feature set apDataCollection, saved
Jul 5, 2026 5:04:59 PM
Stop AP statistics collection on WLC with IP address 10.127.197.194 with data saved into file bootflash
Jul 5, 2026 5:10:00 PM
Stop data collection on COS AP with IP address 10.127.197.180 over SSH for feature set apDataCollection
Jul 5, 2026 5:10:01 PM
Start AP show-tech wireless collection on WLC with IP address 10.127.197.194 for AP name LAB-9115 and s
Jul 5, 2026 5:10:02 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:10:07 PM
Check if bootflash:<file-name>is present and its data collection is complete on WLC with IP address 10.
Jul 5, 2026 5:10:15 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:10:20 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:10:27 PM
Check if bootflash:<file-name>is present and its data collection is complete on WLC with IP address 10.
Jul 5, 2026 5:10:34 PM
Stop AP show-tech wireless collection on WLC with IP address 10.127.197.194 with data saved into file b
Jul 5, 2026 5:10:35 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19
Jul 5, 2026 5:10:36 PM
Check if file bootflash:<file-name>has been uploaded successfully from WLC with IP address 10.127.197.1
Jul 5, 2026 5:10:41 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.
Jul 5, 2026 5:10:41 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:10:41 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
Jul 5, 2026 5:10:43 PM
Stop RA Trace for AP: <MAC>
Jul 5, 2026 5:10:46 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
```

```
Jul 5, 2026 5:10:49 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:10:53 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:10:57 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:11:02 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19
Jul 5, 2026 5:11:03 PM
Check if file bootflash:<file-name> log has been uploaded successfully from WLC with IP address 10.127.
Jul 5, 2026 5:11:08 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.
Jul 5, 2026 5:11:08 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:08 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
Jul 5, 2026 5:11:10 PM
Stop RA Trace for AP: <MAC>
Jul 5, 2026 5:11:13 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:11:15 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:11:19 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:11:22 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:11:27 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:11:30 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19
Jul 5, 2026 5:11:32 PM
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.
Jul 5, 2026 5:11:37 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.
Jul 5, 2026 5:11:37 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:39 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
Jul 5, 2026 5:11:41 PM
Stopping PCAP <file-name> session with <AP-MAC> filter on TenGigabitEthernet0/0/7 interface.
Jul 5, 2026 5:11:41 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19
Jul 5, 2026 5:11:41 PM
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.
Jul 5, 2026 5:11:46 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.
Jul 5, 2026 5:11:53 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:11:56 PM
```

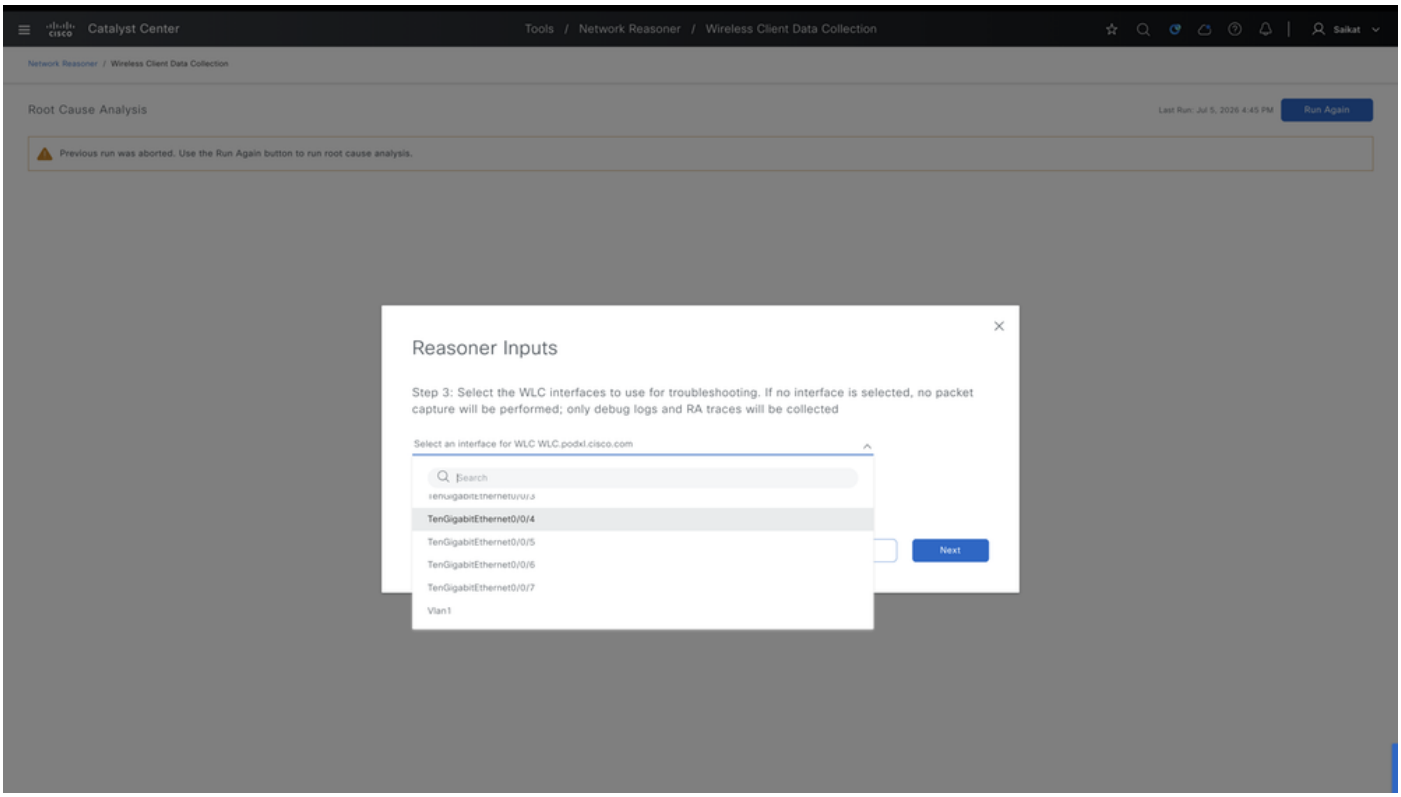
3. Clients sans fil : si un utilisateur rencontre des problèmes Wi-Fi, sélectionnez le contrôleur sans fil auquel il est connecté, saisissez l'adresse MAC de son périphérique et choisissez la durée de surveillance de l'outil. Elle permet de consulter les journaux de statistiques, les suivis RA et la capture de paquets pour voir les données réelles échangées. Voici le workflow d'activation de Network Reasoner pour le client sans fil, ainsi que les résultats correspondants :



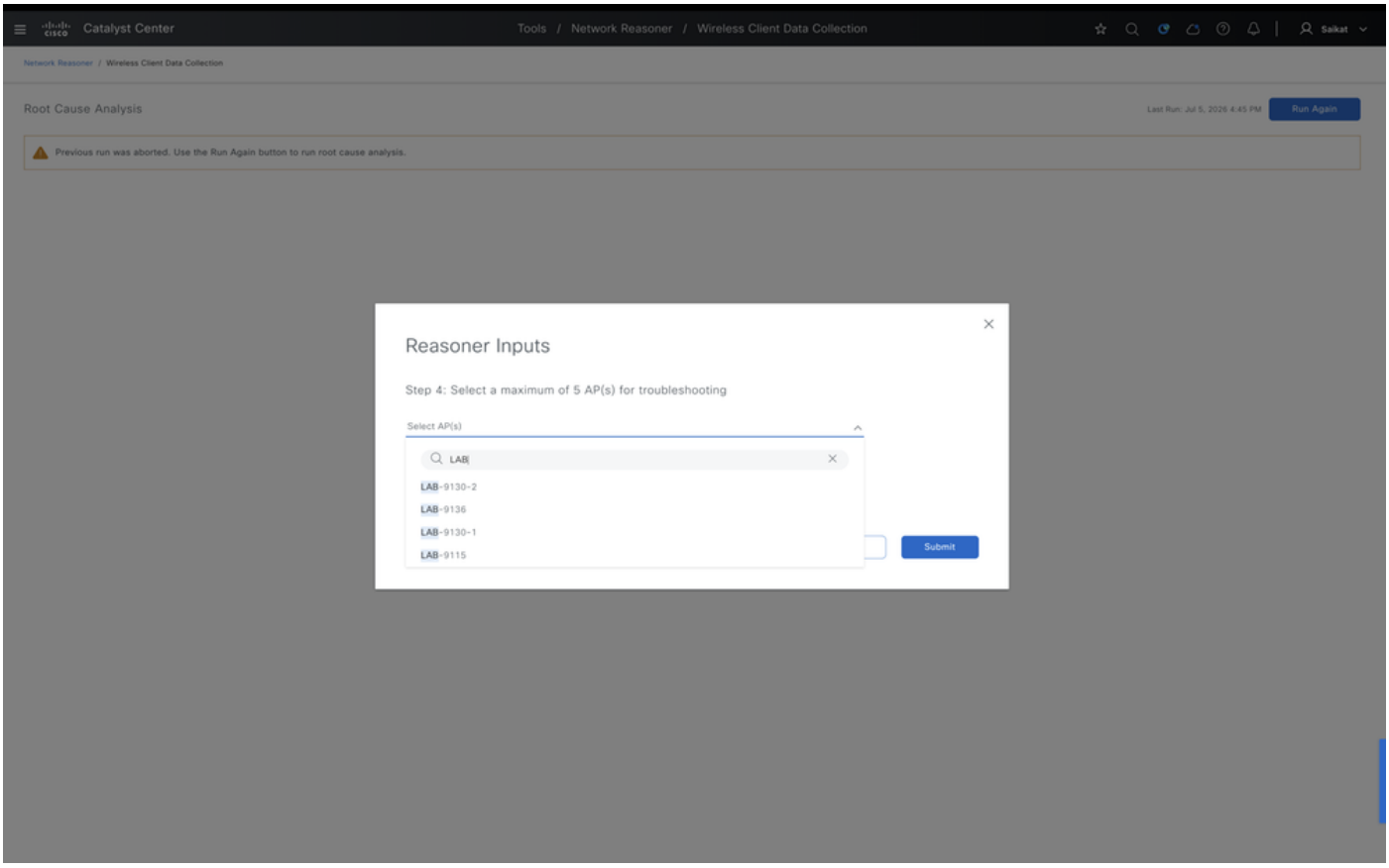
Fournir les détails du client pour le dépannage



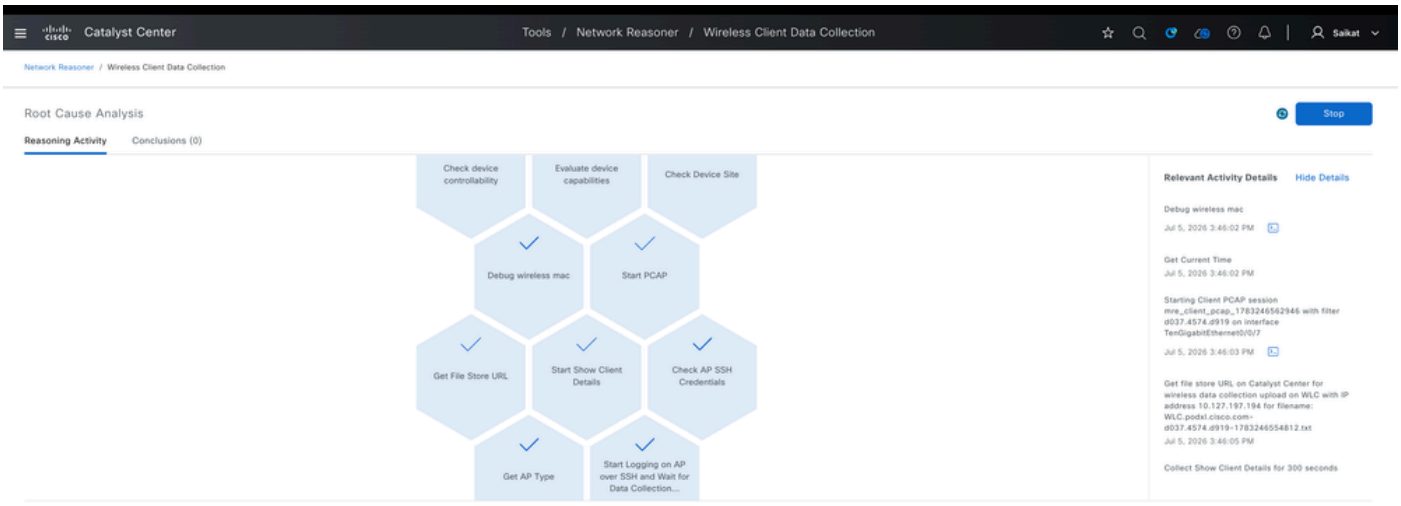
Sélectionnez WLC pour dépanner les adresses MAC client sans fil



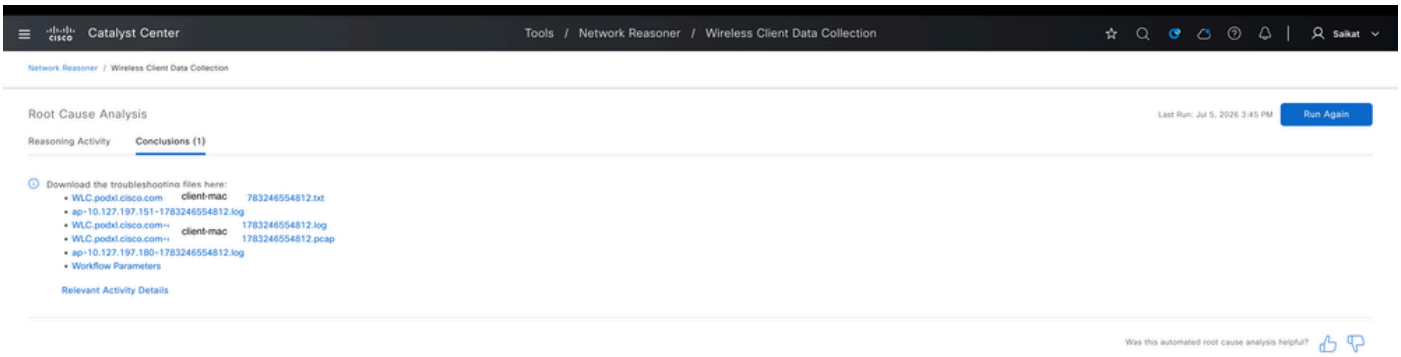
Sélectionnez Interface sur WLC pour dépanner le client sans fil



Sélectionnez les points d'accès (4 max.) pour dépanner le client sans fil



Tâches en cours pour dépanner un problème de client sans fil



Captures collectées à partir du WLC et du point d'accès pour problème client sans fil

```
!! Task Workflow !!
Get Current Time
Jul 5, 2026 5:53:11 PM
Check device controllability
Jul 5, 2026 5:53:11 PM
Determine if device is reachable
Jul 5, 2026 5:53:11 PM
Determine if the network features are supported on the given wireless platform
Jul 5, 2026 5:53:11 PM
Check if the device <device> is provisioned or assigned to a site.
Jul 5, 2026 5:53:12 PM
Debug wireless mac
Jul 5, 2026 5:53:18 PM
Get Current Time
Jul 5, 2026 5:53:19 PM
Starting Client PCAP session <file-name> with filter <clien-mac> on interface TenGigabitEthernet0/0/7
Jul 5, 2026 5:53:20 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
Jul 5, 2026 5:53:21 PM
Collect Show Client Details for 300 seconds
Jul 5, 2026 5:53:22 PM
Check if AP with IP address 10.127.197.180 has SSH credentials configured in Catalyst Center
```

```
Jul 5, 2026 5:53:24 PM
Get type of AP with IP address 10.127.197.180
Jul 5, 2026 5:53:25 PM
Start logging on COS AP with IP address 10.127.197.180 over SSH for Client MAC <client-mac> feature set
Jul 5, 2026 5:53:28 PM
End Show Client Details
Jul 5, 2026 5:58:35 PM
Stop data collection on COS AP with IP address 10.127.197.180 over SSH for Client MAC <client-mac> featu
Jul 5, 2026 5:58:36 PM
Stop data collection on COS AP with IP address 10.127.197.151 over SSH for Client MAC <client-mac> featu
Jul 5, 2026 5:58:38 PM
Check File Size: <file-name>
Jul 5, 2026 5:58:38 PM
Start to upload file <file-name> from WLC with IP address 10.127.197.194 to https://10.105.193.40/api/v1
Jul 5, 2026 5:58:40 PM
Check if file <file-name> has been uploaded successfully from WLC with IP address 10.127.197.194 to http
Jul 5, 2026 5:58:45 PM
File <file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.105.193.40/
Jul 5, 2026 5:58:45 PM
Delete the file <file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:58:45 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
Jul 5, 2026 5:58:47 PM
No debug wireless mac
Jul 5, 2026 5:58:49 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:58:52 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:58:56 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:58:59 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:59:03 PM
Check if bootflash:<file-name> is present and its data collection is complete on WLC with IP address 10
Jul 5, 2026 5:59:07 PM
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19
Jul 5, 2026 5:59:09 PM
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.
Jul 5, 2026 5:59:14 PM
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to https://10.
Jul 5, 2026 5:59:14 PM
Delete the file bootflash:<file-name> from WLC with IP address 10.127.197.194
Jul 5, 2026 5:59:14 PM
Get file store URL on Catalyst Center for wireless data collection upload on WLC with IP address 10.127
```

5 juil. 2026 17:59:16

```
Stopping PCAP <file-name> session with d037.4574.d919 filter on TenGigabitEthernet0/0/7 interface.
```

5 juil. 2026 17:59:16

```
Check File Size:bootflash:<file-name>
```

5 juil. 2026 17:59:16

```
Start to upload file bootflash:<file-name> from WLC with IP address 10.127.197.194 to https://10.105.19
```

5 juil. 2026 17:59:18

```
Check if file bootflash:<file-name> has been uploaded successfully from WLC with IP address 10.127.197.
```

5 juil. 2026 17:59:23

```
File bootflash:<file-name> uploaded successfully from WLC with IP address 10.127.197.194 to
```

5 juil. 2026 17:59:23
Supprimez le fichier bootflash:<nom-fichier> du WLC avec l'adresse IP 10.127.197.194
5 juil. 2026 17:59:23

Références techniques

- Guide de déploiement de Cisco Intelligent Capture
- Gérer les captures intelligentes
- Guide de l'utilisateur de Cisco Catalyst Assurance, version 2.3.7.x
- Dépannage d'un périphérique réseau à l'aide de Network Reasoner - HA sur un contrôleur LAN sans fil à l'aide du workflow MRE

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.