



Cisco Aironet センサー導入ガイド

[Cisco Aironet センサー導入ガイドの概要](#) 2

[センサーとしてのアクセス ポイント](#) 2

[ソフトウェアの最小要件](#) 8

[DNAC 設定の要件](#) 8

[センサー データ フロー](#) 14

[センサーを DNAC に追加する](#) 15

[テストスイートの作成](#) 17

[AP センサーと AP-1800s の違い](#) 21

[DNAC ディスカバリの有効化](#) 22

[トラブルシューティング コマンド](#) 26

[参考 URL](#) 31

改訂：2018年12月3日

Cisco Aironet センサー導入ガイドの概要

数年前までは、ワイヤレス ネットワークは会議室や共用スペースの利便性の向上のためのみに使用されていました。現在、ワイヤレス LAN は企業ネットワークの設備全体で標準的に使用されているだけでなく、かつてないほど重要な意味を持っています。これは、多くの企業がイーサネットから完全なワイヤレスのみのインフラストラクチャに移行しているためです。

このようなワイヤレス ネットワークは、IT 専門家が常駐できない遠隔地の施設で特に発展しており、潜在的な接続性の問題を、ユーザが接続性の低下を訴えたりこれに気付いたりする前に、迅速に特定して解決できる能力が重要になっています。

これらの問題に対処するために、シスコのワイヤレス サービス アシユアランスおよび「センサー」モードと呼ばれる新しい AP モードが導入されました。シスコのワイヤレス サービス アシユアランス プラットフォームは、ワイヤレス パフォーマンス分析、リアルタイム クライアント トラブルシューティング、およびプロアクティブな健全性アセスメントの3つのコンポーネントで構成されています。サポートされている AP または専用センサーを使用することで、デバイスは実際に WLAN クライアントのように機能し、IT 専門家や技術者を常駐させなくてもネットワーク内のクライアント接続性の問題をリアルタイムで関連付けおよび特定します。

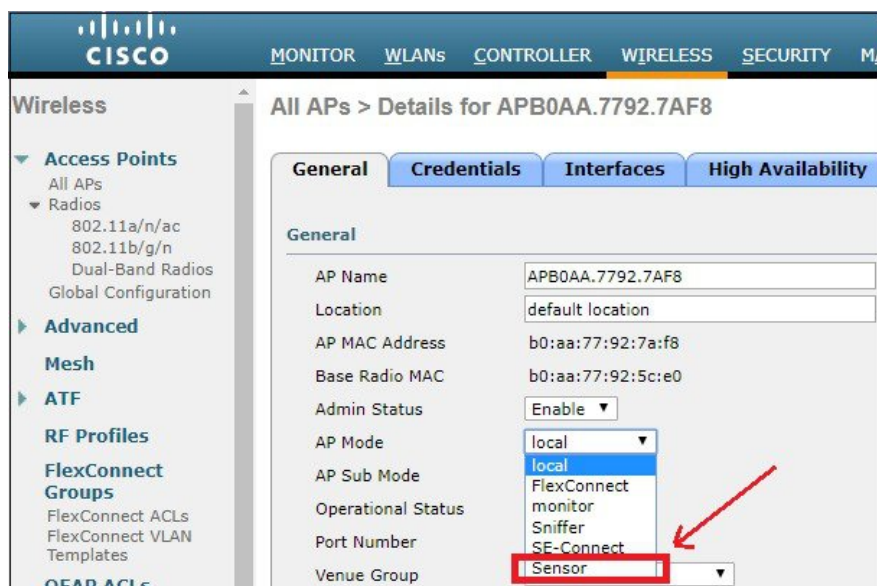
このドキュメントは、センサーとしての Cisco 1815i、1830、1850、2800 & 3800 シリーズ アクセス ポイント、およびスタンドアロン Cisco Aironet 1800s ワイヤレス ネットワーク センサーを対象にしています。

Cisco Aironet 1800s ワイヤレス ネットワークのセンサーは、シスコのワイヤレス サービス アシユアランス ソリューションの一部です。

センサーとしてのアクセス ポイント



シスコアクセス ポイント モデル AP-1815、1830、1850、2800、3800 シリーズは、専用センサーとして機能できます。これは、コントローラ上で AP モードが「センサー」としてリストされる新しい AP モードタイプです。



センサーモードでは、アクセスポイント内部の無線は、ネットワークへの接続を確立するクライアントのように機能します（WLANクライアントとして）。これにより、以下のテストや機能を実行できるようになります。

- ネットワーククライアント接続オンボーディングテスト
 - 802.11 アソシエーション
 - 802.11 認証と鍵交換
 - IP アドレッシング DHCP (IPv4)
- 一般的なネットワークテスト
 - DNS (IPv4)
 - RADIUS (IPv4)
 - ファーストホップルータ/デフォルトゲートウェイ (IPv4)
 - イン트라ネットホスト
 - 外部ホスト (IPv4)
- クライアントアプリケーションテスト
 - 電子メール：POP3、IMAP、Outlook Web Access (IPv4)
 - ファイル転送：FTP (IPv4) アップロードおよびダウンロード
 - Web：HTTP および HTTPS (IPv4)




(注) AP-1815i、1830およびAP 1850モデルがセンサーモードの場合、APがクライアントにサービスを提供する機能は無効化されます。これらのモデルでは、同時に1つのモードでしか動作できません（センサーまたはAP）。



(注) APがセンサーとして接続されている場合は、クライアントのように接続します。RFの問題がある場合、APはクライアントがAPにアクセスして、このトラフィックをDNCに渡すことを許可します。

Cisco Aironet 1800s Wireless Network Sensor



Cisco Aironet® 1800 Series

- Full DNA Assurance Sensor Support
- 2x2 with 2 spatial streams
- 802.11ac Wave 2
- Multiple powering options:
 - PoE Power
 - USB Type “C” power
 - Direct AC Power Plug
- Integrated BLE
- Small form-factor(WxLxH) :
 - 3.25” x 4.75” x 0.75”

Cisco Aironet AP-1800シリーズは、非常に小さなフォームファクタの専用センサーです。センサーに挿入される小型のスライドモジュールにより、さまざまな方法で電源を供給できます。

PoEモジュールを使用しない場合、ローカルの5ボルトUSB電源を使用できます。PoE動作の他に、AC電源を直接使用できるモジュールがあります。

AP1800s inside view (backside)



85mm

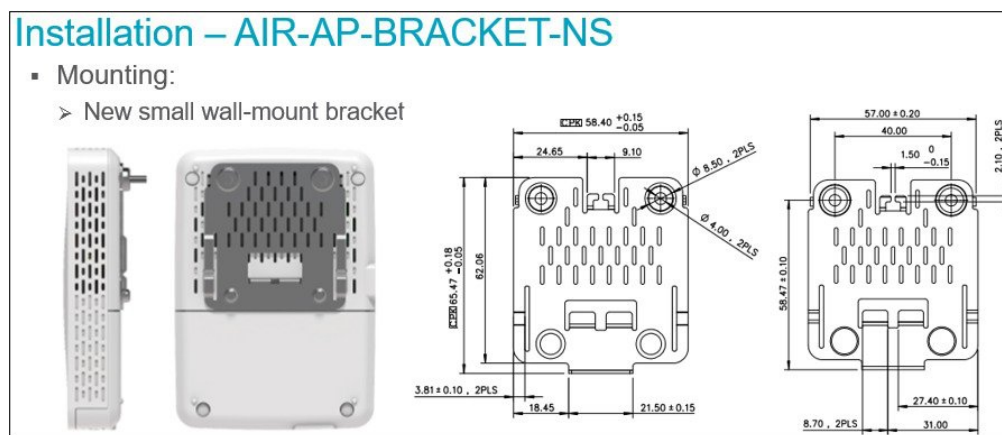
119mm

24mm

Optional Powering Options

- AIR-MOD-AC-US**
- AIR-MOD-POE**
- AIR-MOD-USB**

センサーはサイズが小さいため（アクセスポイントよりかなり小さい）、壁面取り付けが必要な場合は、このセンサーに小型ブラケット シスコ部品番号 AIR-AP-BRACKET-NS を使用できます。



センサー内蔵の 2.4 GHz および 5 GHz 無線に加え、専用 Bluetooth Low Energy 無線も組み込まれており、将来 BLE アプリケーションに使用することができます。

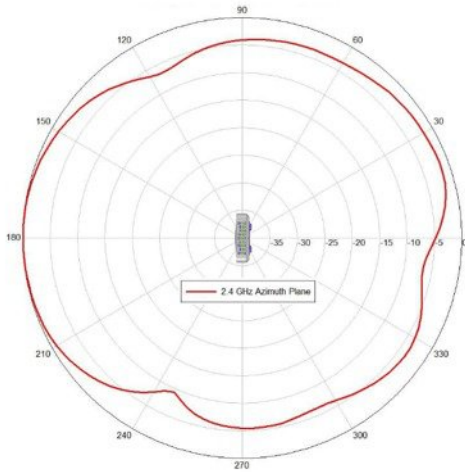
AP 1800s センサーのアンテナ システムの詳細を示します。

AP1800s Antenna System

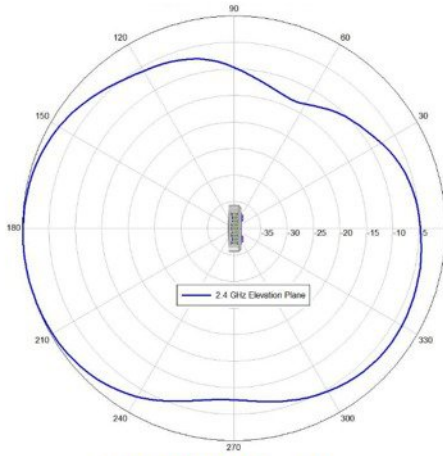
AP1800s	Wi-Fi Antenna Specs	Bluetooth Antenna Specs
Frequency Range	2.4 - 2.5 GHz & 5.15 - 5.925 GHz	2.4 - 2.5 GHz
Gain	3 dBi @ 2.4 GHz/5 dBi @ 5 GHz	1 dBi
Polarization	Elliptical	Elliptical
Antenna Connector	Integrated	Integrated
Mounting	Integrated	Integrated
Antenna Type	Dual-Band Monopoles	Monopole

デュアルバンドアンテナ（垂直偏波）がセンサーの側面にあり、BLE アンテナは、センサーのプリント基板に取り付けられています。

AP1800s Antenna Patterns 2.4 GHz

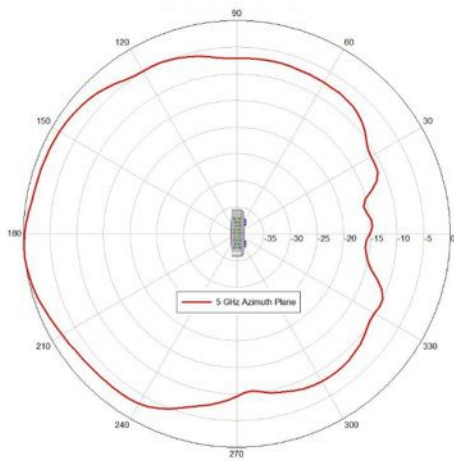


2.4 GHz Azimuth

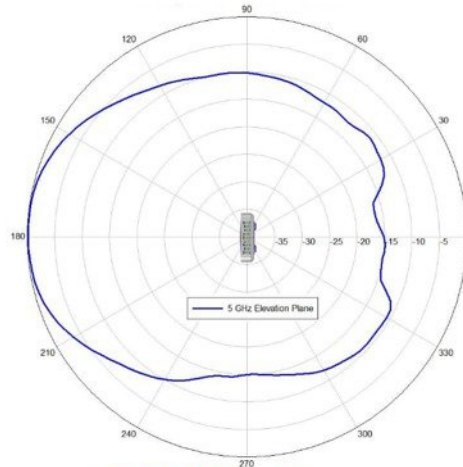


2.4 GHz Elevation

AP1800s Antenna Patterns 5 GHz

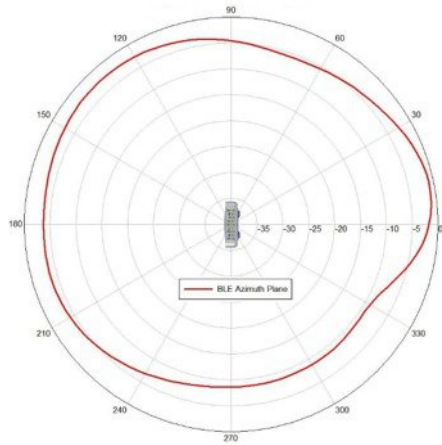


5 GHz Azimuth

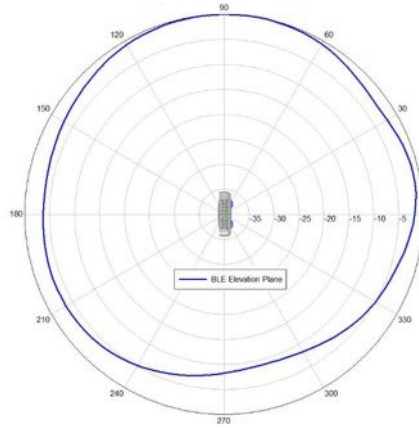


5 GHz Elevation

AP1800s Antenna Patterns Bluetooth Low Energy



2.4 GHz BLE Azimuth



2.4 GHz BLE Elevation

AP1800s Console Port

- RJ45 console adapter via 4-pin polarized connector
 - Rx, Tx, GND, 3.3V power
- Same pinout as the AP1815w
- AIR-CONSADPT=
 - Orderable PID



AP1800s PIDS



Name	PID
Network Sensor Client,	AIR-AP1800S-x-K9
USB Adapter Power Module – US plug only	AIR-MOD-USB-US(=)
USB Adapter Power Module – Rest of World (includes bag of 5 international plugs)	AIR-MOD-USB-RW(=)
PoE Adapter Power Module	AIR-MOD-POE(=)
Wall mount bracket kit (includes screws)	AIR-AP-BRACKET-NS
AC Adapter Power Module-US,	AIR-MOD-AC-US(=)
AC Adapter Power Module-EU,	AIR-MOD-AC-EU(=)
AC Adapter Power Module-UK,	AIR-MOD-AC-UK(=)
AC Adapter Power Module-AU,	AIR-MOD-AC-AU(=)
AC Adapter Power Module-CH,	AIR-MOD-AC-CH(=)
AC Adapter Power Module-SA,	AIR-MOD-AC-SA(=)

ソフトウェアの最小要件

- WLC ソフトウェア バージョン **8.5MR2**
- DNA Center アプライアンス **1.1.1**
- DNAC 「アシュアランス - センサー」 パッケージのバージョン**1.0.5.301**

DNAC 設定の要件

DNAC でセンサーを設定する前に、WLC がブラウフィールドアシュアランス用に追加されている必要があります。これを確認するには、WLC で「**show network assurance summary**」を実行して、エラーが報告されないこと、および「Last Success」の時刻が最近のものであることをチェックします。

アシュアランス用の WLC を追加するには、次の 4 つの手順に従います。

1. サイト、建物、フロアの階層を作成する
2. センサー プロファイルを作成し、センサーを要求する
3. デバイス クレデンシャルを追加して、WLC のディスカバリを実行する
4. WLC をサイトにプロビジョニングする
5. 検出された AP をフロアに割り当てる

1. サイト、建物、フロアの階層を作成する

DNA Center のメイン画面で、[Design] アイコンの下の [Add site locations on the network] リンクを選択します。

What can DNA Center do?

Design

Model your entire network, from sites and buildings to devices and links, both physical and virtual, across campus, branch, WAN and cloud.

- [Add site locations on the network](#)
- [Designate golden images for device families](#)
- [Create wireless profiles of SSIDs](#)

次に [Add Site] を選択して、環境の必要に応じてサイト、建物、フロアを作成します。

Add Site ✕

Area contains other areas and/or buildings. Buildings contain floors and floor plans.

Area Building

Site Name*
eg : San jose

Parent
Global ▼

Or select a file

[Upload CSV](#)


[Download Template](#)

2. デバイスのクレデンシャルを追加して、ディスカバリを実行する

WLCのデバイスクレデンシャルを追加して、DNACでネットワークアシュアランスサービスの設定および有効化を可能にし、WLCに接続しているデバイスとクライアントを学習できるようにする必要があります。SNMPRWおよびCLIのクレデンシャルを、下に示す **[Design] > [Network Settings] > [Device Credentials]** タブに入力します。

デバイス クレデンシヤルを追加したら、ディスカバリが実行されて WLC が検出されます。DNAC のメイン ページで [Discovery] アイコンを選択し、WLC の必要な IP 詳細情報を入力して、以前に追加したクレデンシヤルを選択 します。

Tools



Discovery

Automate addition of devices to controller
inventory

The screenshot displays the Cisco DNA Center Discovery interface. On the left, there is a sidebar with 'Discoveries' and a search bar. The main area is titled 'New Discovery' and contains the following fields:

- Discovery Name***: A text input field with a search icon.
- IP ADDRESS/RANGE**: A section with a dropdown menu set to 'CDP' and a 'Range' button.
- IP Address***: A text input field.
- Subnet Filters**: A text input field with a plus sign.
- CDP Level**: A dropdown menu set to '16'.
- Preferred Management IP**: A dropdown menu set to 'None'.

Below the form, there is a 'CREDENTIALS*' section with an 'Add Credentials' button and a legend for 'GLOBAL' (blue) and 'JOB SPECIFIC' (yellow). A table below shows four credential types, each with 'No credentials to display':

CLI	SNMPV2C READ	SNMPV2C WRITE	SNMP V3
No credentials to display	No credentials to display	No credentials to display	No credentials to display


3. WLC をサイトにプロビジョニングする

次に、WLC と AP をサイトとフロアに割り当てます。DNAC メインページの [Provision] アイコンの下の [Provision WLCs and APs to defined sites] リンクを選択します。

The screenshot shows the 'Provision' page in Cisco DNA Center. It includes a gear icon and the heading 'Provision'. The text below reads: 'Provide new services to users with ease, speed and security across your enterprise network, regardless of network size and complexity.' Below this are three bullet points:

- Discover and provision switches to defined sites
- Provision WLCs and APs to defined sites
- Set up Campus Fabric across switches

このページで、WLC および AP の横にあるチェックボックスをオンにして [Assign Device to Site] を選択し、デバイスを建物やフロアに割り当てます。WLC は建物に割り当てられ、AP はフロアに割り当てられるようにします。


DESIGN
POLICY
PROVISION
ASSURANCE

Devices

Device Inventory

Inventory (100) Unclaimed Devices (0)

Filter | Actions

<input type="checkbox"/>	Device Name	Type	IP Address	Site
<input checked="" type="checkbox"/>	AP00D7.8		192.168.0.186	
<input checked="" type="checkbox"/>	KLNK01-SENS3-1815I	Unified AP	10.40.100.134	
<input checked="" type="checkbox"/>	STUB01-A0	Unified AP	10.40.100.5	
<input checked="" type="checkbox"/>	STUB01-A1	Unified AP	10.40.100.12	

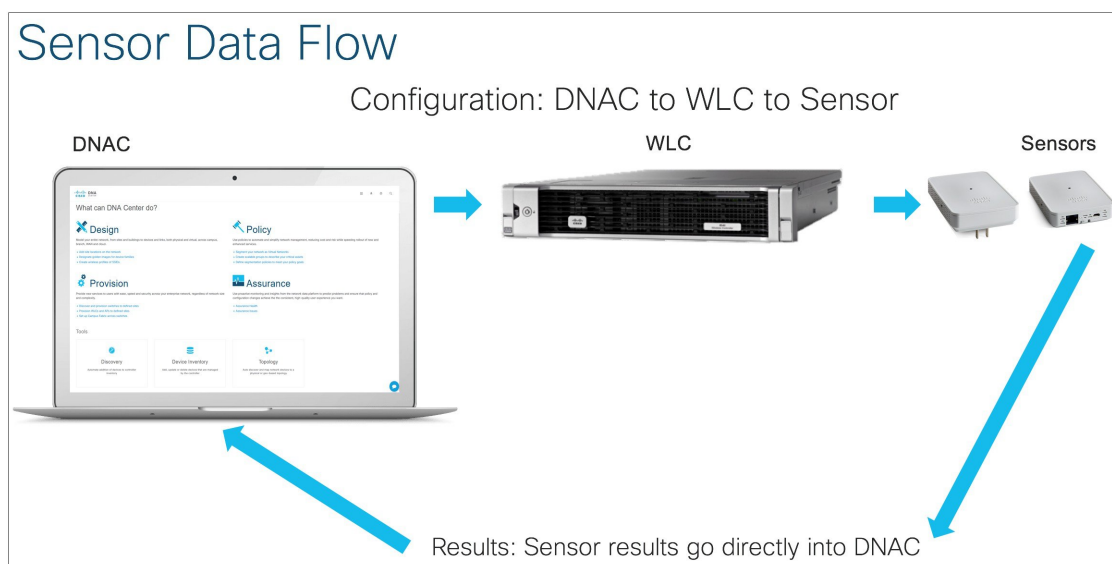
次の4つの手順に従って、APをフロア上に配置します（オプション）。



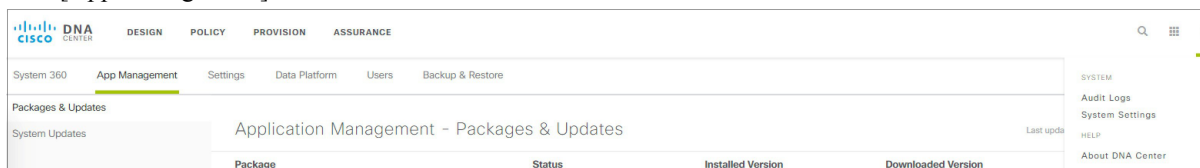
これで DNAC がアシュアランス用にセットアップされ、AP がフロア プラン上に配置されました。

センサー データ フロー

センサーとして機能している場合、センサー AP はテストスイート構成が DNAC 内で作成された後に、WLC からこれを受信します。ただし、実際のテスト結果は WLC をトラバースしません。これらは、センサーから DNAC に直接送信されます。



DNA Center では、システムがオンラインで初期構成が完了した時点でセンサー パッケージがインストールされている必要があります。「アシュアランス-センサー」パッケージが、アプリケーション管理カタログからインストールされている必要があります。これを行うには、DNAC にログインして右上の歯車アイコンを選択して [System Status] を選択し、[App Management] タブを選択します。

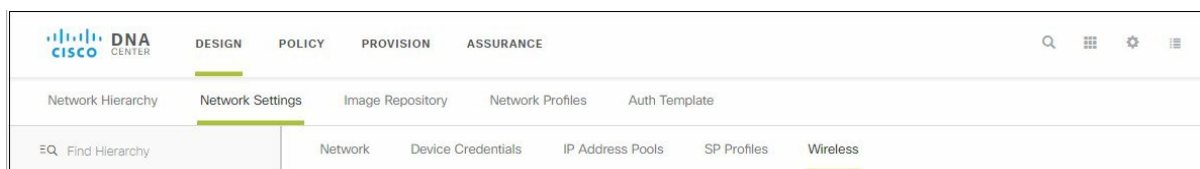


[Application Management - Packages & Updates] ページが表示され、「アシュアランス-センサー」パッケージが一覧表示されます。[Install] リンクをクリックして、センサー パッケージのインストールを開始します。完了するまで最大 40 分かかる場合があります。

センサーを DNAC に追加する

センサーがネットワークを介して DNAC に到達可能であることを確認します。センサーは、有線の場合とワイヤレスの場合があります。センサーがワイヤレスの場合は、後述の「イーサネットを使用しない 1800s センサーのプロビジョニング」セクションの手順に従って、ネットワークを準備してください。センサーが有線の場合は、有線ネットワーク経由で DNAC に到達可能であることを確認してください。

次に DNAC でセンサー プロファイルを作成する必要があります。[Design] > [Network Settings] > [Wireless] に移動して、表示されたウィンドウで [Sensor Settings] まで下にスクロールします。



次に [Add] ボタンをクリックして、[Settings Name] と [Wireless network SSID] を指定し、適切なセキュリティ設定を構成します。プロファイルを保存します。注：ワイヤレス ネットワーク SSID は、WLC で設定されたバックホール設定と一致するバックホール SSID です。WLC でバックホールを設定する手順については、「バックホール設定」セクションを参照してください。

Settings Name *
backhaul_profile

Wireless Network Name (SSID) *
backhaul

LEVEL OF SECURITY *

WPA2 Enterprise WPA2 Personal Open

Secure
A password (Pre-shared key PSK with WPA2 encryption) is needed to access the wireless network.

Password*
.....

Cancel Save

次に、デバイスを要求する必要があります。ネットワークを介してセンサーがDNACに到達可能な場合、デバイスは要求元不明デバイスのリストに表示されます。[Provision] > [Unclaimed Devices] に移動します。

Device Inventory

Inventory **Unclaimed Devices (2)**

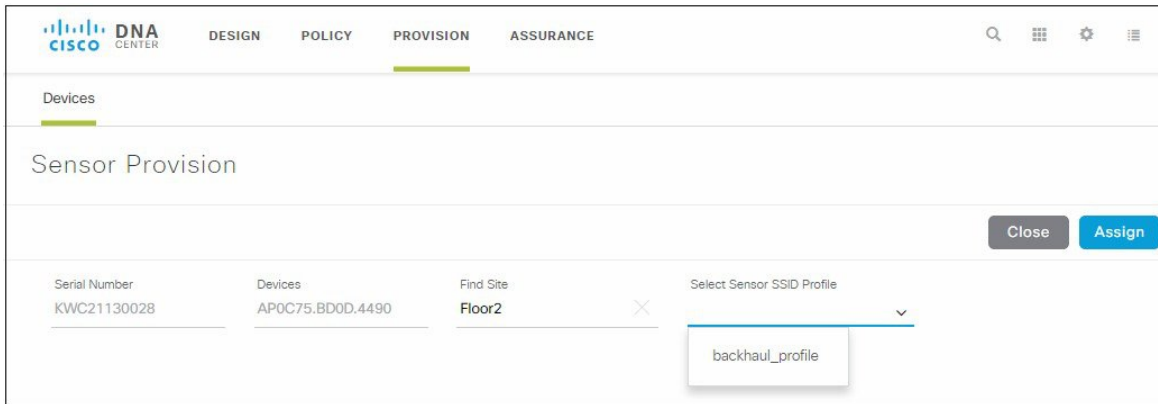
Refresh

Filter | Claim Device Delete Device Sensor Provision

Device Name	Serial Number	Product ID	IP Address	Location	OS Image	Uptime	First Seen	Status	
<input type="checkbox"/>	AP0C75.BD09.5CF8	RFDP2BFA027	AIR-AP1800S-B-K9	20.20.0.52	Unassigned	cheetah	2018-01-26 18:07:56.000581	2018-01-26 06:14:51.000665	UNCLAIMED
<input checked="" type="checkbox"/>	AP0C75.BD0D.4490	KWC21130028	AIR-AP1800S-B-K9	20.20.0.67	Unassigned	cheetah	2018-01-26 18:06:50.000336	2018-01-25 18:18:30.000061	UNCLAIMED

Show 10 entries Showing 1 - 2 of 2 Previous 1 Next

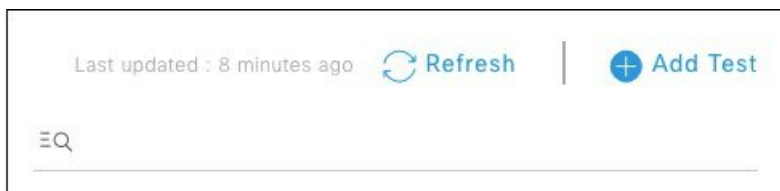
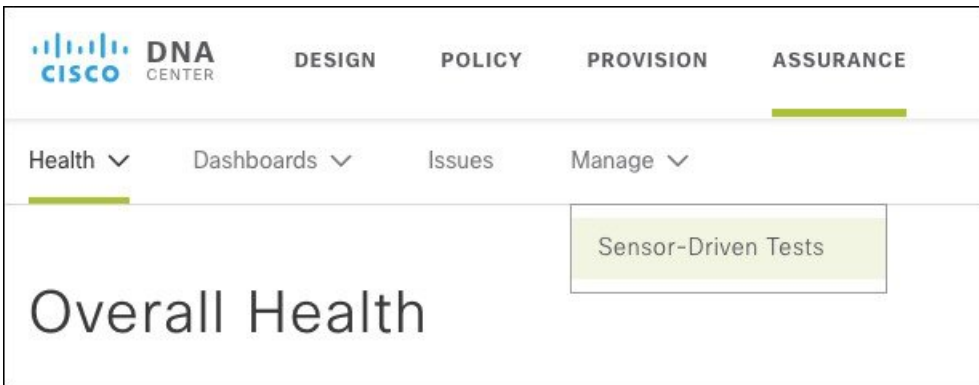
要求元不明デバイスのリストでセンサーを選択して、[Sensor Provision] をクリックします。次に、フロアにセンサーを追加し、センサーのプロファイルを選択する必要があります。



これで、センサーはプロビジョニングされ、完了後にインベントリに表示されます。管理対象状態になっている場合、テストスイートをセットアップする準備ができています。

テストスイートの作成

センサーパッケージをインストールしたら、[DNA Assurance] > [Manage] > [Sensor Driven Tests] に移動して、[Add Test] を選択してテストスイートの作成を開始します。



手順

- ステップ 1** テスト名、ロケーション、およびテストを実行する頻度を、[Add Test] ページで定義します。
テストは、30 分間隔または 1 時間間隔で実行することが推奨されます。

Test Name	Location	Interval-Hours
		Every 30 Minutes
		Daily: <input checked="" type="radio"/> Every <input type="text" value="30"/> Minut... Once: <input type="radio"/> Exactly At 01 / 08 / 2018 12 : 00 : AM

ロケーションを選択するとき、該当フロアにブロードキャストされている SSID が、[Test Name]、[Location]、[Interval-Hours] の各フィールドの下に表示されます。SSID とバンドを1つのみ選択します。各 SSID および各バンドに対して、追加のテストを作成します。WPA2_EAP（EAP-FAST および PEAP MSCHAPv2）、PSK、および Open の各認証モードが現在サポートされています。SSID を選択して認証の詳細を入力したら、次に進みます。

SSID	Radios To Test	Security	Credentials		
			User Name	Password	EAP Method
eduroam	<input type="checkbox"/> 2.4 GHz <input type="checkbox"/> 5 GHz	WPA2_EAP			
ShawOpen	<input type="checkbox"/> 2.4 GHz <input type="checkbox"/> 5 GHz	OTHER			

ステップ 2 センサーで実行するテストを選択します。

ネットワークテスト、RADIUS テスト、およびアプリケーションテスト（電子メール、Web、FTP を含む）を選択できます。

下のスクリーンショットは、実行可能なテストの完全なリストを示しています。

Network Tests

IP Addressing Tests

DHCPv4

DNS Tests

DNS (IPv4)

Hostname to resolve

Host Reachability Tests

User Defined Host (IPv4)

Internal IP Address _____ External IP Address _____ +

Default Gateway Reachability (IPv4)

RADIUS Tests

RADIUS Server (IPv4)

IP Address / Hostname _____ User Name _____

Shared Secret _____ Password _____

Port _____ Protocol _____

Application Tests

Email Tests

POP3 (IPv4)

Enter POP3 Server _____ +

IMAP (IPv4)

Enter IMAP Server _____ +

Outlook Web Access (IPv4)

URL _____ User Name _____

Password _____ +

Web Tests

HTTP (IPv4)

Enter URL _____ +

File Transfer Tests

FTP (IPv4)

Server Name _____ User Name _____

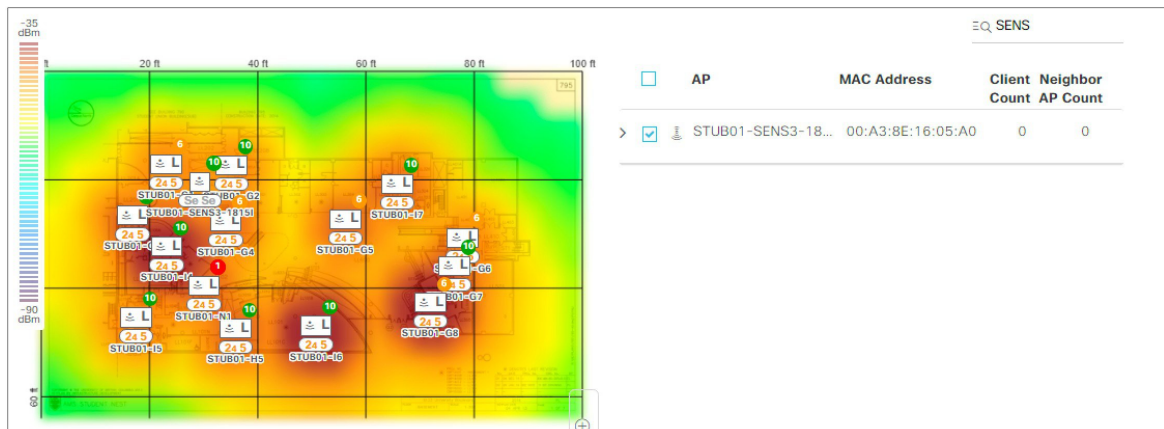
Password _____ Protocol ftp

Transfer Tune _____ Download File Path/Upload Path _____ +

DHCPv4、DNS、およびホスト到達可能性のテストを含む最小限のテストスイートで開始することをお勧めします。これらのテストが成功したら、テストスイートを変更してRADIUSまたはその他のアプリケーションをテストします。[Next] をクリックして、テストスイートの追加の最終ステップに進みます。

ステップ3 センサーを選択します。

これは、周囲の領域の AP をテストするためにセンサーモードに変換される AP です。このセンサーは、RSSI カットオフ値 -75 で受信可能なすべての AP をテストします。



センサーを選択したら、[Save] をクリックします。AP は、センサー モードに変換されます。AP のモードが変更されると、画面の上部にメッセージが表示されます。これは、初めてテストが追加されて AP モードが変更されたときのみ行われます。



新しく追加されたテストが、[Sensor-Driven Tests] ページが表示されます。テストの概要が表示され、[View] を選択するとテスト結果の詳細が表示されます。

Sensor-Driven Tests

Last updated : in a few seconds [Refresh](#) | [+ Add Test](#)

EQ

Test Name	Location	Schedule	SSIDs	Test Types	Test Results			Last Run	Actions				
					Last 24 hours	Latest	Details						
eduroam-5ghz	Site-UBC / Student Nest / Floor 0	Daily, every 30 MINUTES	eduroam	Onboarding Test IP Addressing Test DNS Test Host Reachability Test Web Server Test						None None None None None	View	-	⋮

ステップ 4 [View] を選択すると、センサーがテストを実行したすべての AP と、これらのテストの結果がリストされます。

センサー名、SSID、および AP 名が示され、テスト タイプと結果が表示されます。

Sensor Name	Sensor Type	SSID	Band	APs	Test Type	Result	Test Time
STUB01-SENS3-1815I	Ap-As-Sensor	eduroam	2.4 GHz 5 GHz	STUB01-L3	Onboarding Test IP Addressing Test Web Server Test	Failed None None	01/09/18 10:47 AM
STUB01-SENS3-1815I	Ap-As-Sensor	eduroam	2.4 GHz 5 GHz	STUB01-G0	Onboarding Test IP Addressing Test Web Server Test	Failed None None	01/09/18 10:45 AM
STUB01-SENS3-1815I	Ap-As-Sensor	eduroam	2.4 GHz 5 GHz	STUB01-A9	Onboarding Test IP Addressing Test Web Server Test	Passed Passed Failed	01/09/18 10:43 AM
STUB01-SENS3-1815I	Ap-As-Sensor	eduroam	2.4 GHz 5 GHz	STUB01-L1	Onboarding Test IP Addressing Test Web Server Test	Passed Passed Failed	01/09/18 10:43 AM
STUB01-SENS3-1815I	Ap-As-Sensor	eduroam	2.4 GHz 5 GHz	STUB01-N1	Onboarding Test IP Addressing Test Web Server Test	Passed Passed Failed	01/09/18 10:43 AM

AP センサーと AP-1800s の違い

Cisco Aironet AP-1800s は、非常に小さなフォーム ファクタの専用センサー無線機器です。これは専用センサーとしてのみ機能し、プラグアンドプレイを使用して DNAC（センサーパッケージ）を検出するため、コントローラに参加しません。



(注) プラグ アンド プレイは、アクセス ポイントの場合は WLC オンボーディングで発生します。

プラグ アンド プレイは、アクセス ポイントの場合は WLC オンボーディングで発生します。

イーサネットを使用しない 1800s センサーのプロビジョニング。

1800s センサー（イーサネットモジュールなし）を使用する場合、センサーは次のスクリーンショットで示すように、暫定 SSID を有効にすることで WLAN 経由でプロビジョニングされます。

The screenshot shows the Cisco configuration page for Backhaul Configuration. Under the '1800s' section, the 'Provisioning' dropdown menu is highlighted with a red box and set to 'Enable'. Other settings include SSID: TFTP and Auth-type: Open. A note below states: '* 1800s Default mode of configuration is PnP'.

プロビジョニングを有効にする（および SSID を TFTP に設定する）と、「CiscoSensorProvisioning」と呼ばれる非表示 WLAN が作成され、センサーは EAP TLS クライアント証明書を使用して参加します。

<input type="checkbox"/>	9	WLAN	webnass_nsk	webnass_nsk	Disabled	[WPA2][Auth(PSK)], Web-Passthrough
<input type="checkbox"/>	10	WLAN			Disabled	[WPA2][Auth(PSK)], Web-Auth
<input type="checkbox"/>	11	WLAN			Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	12	WLAN			Disabled	None
<input checked="" type="checkbox"/>	13	WLAN	CiscoSensorProvisioning	CiscoSensorProvisioning	Enabled	[WPA2][Auth(802.1X)]
<input type="checkbox"/>	14	WLAN	wbauth_ext	wbauth_ext	Disabled	Web-Auth

A red box highlights the row for SSID 'CiscoSensorProvisioning' with the text 'AP-1800s Sensor uses this Provisioning SSID (hidden)' and an arrow pointing to the SSID column.

これにより、センサーは DNAC IP を検出できます。これは、DHCP オプション 43 を使用して、または DNS を介して行われます。

バックホール設定



(注) ワイヤレスバックホールは DNAC 1.2.0 以前ではサポートされていません。

バックホールは、既存の WLAN から選択する必要がある SSID で、DNAC と接続および通信を行うためにワイヤレスセンサーによって使用されます。この方法により、DNAC が有線ネットワークを介して到達不可能な場合に、テスト構成がデバイスにプッシュされたり、テスト結果が DNAC に戻されたりします。

WLC でバックホールを設定するには、UI で [Management] > [Cloud Services] > [Network Assurance] > [Sensor] の順に移動します。バックホール設定がウィンドウの上部に表示されます。SSID 名が既存の WLAN と一致し、セキュリティにも一致していることを確認します。

The screenshot shows the Cisco WLC Management UI. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', 'HELP', 'FEEDBACK', and 'Home'. The left sidebar shows a tree view with 'Management' selected, and sub-items like 'Summary', 'SNMP', 'HTTP-HTTPS', 'IPSEC', 'Telnet-SSH', 'Serial Port', 'Local Management Users', 'User Sessions', 'Logs', 'Mgmt Via Wireless', 'Cloud Services', 'Software Activation', and 'Tech Support'. The main content area is titled 'Backhaul Configuration' and contains the following fields:

- SSID: backhaul
- Auth-type: Psik
- Psk Format: ASCII
- Local Management Users: [masked]
- 1800s Provisioning: Enable
- DHCP Interface: management

A note at the bottom states: * 1800s Default mode of configuration is PnP

DNAC ディスカバリの有効化

DHCP の場合

次の ASCII 文字列でオプション 43 を設定する必要があります。例 5A1N;B2;K4;l<DNAC IP Address>;J80
<DNAC サーバの IP アドレス>;J80

DNS の場合は、2 つのステップがあります。

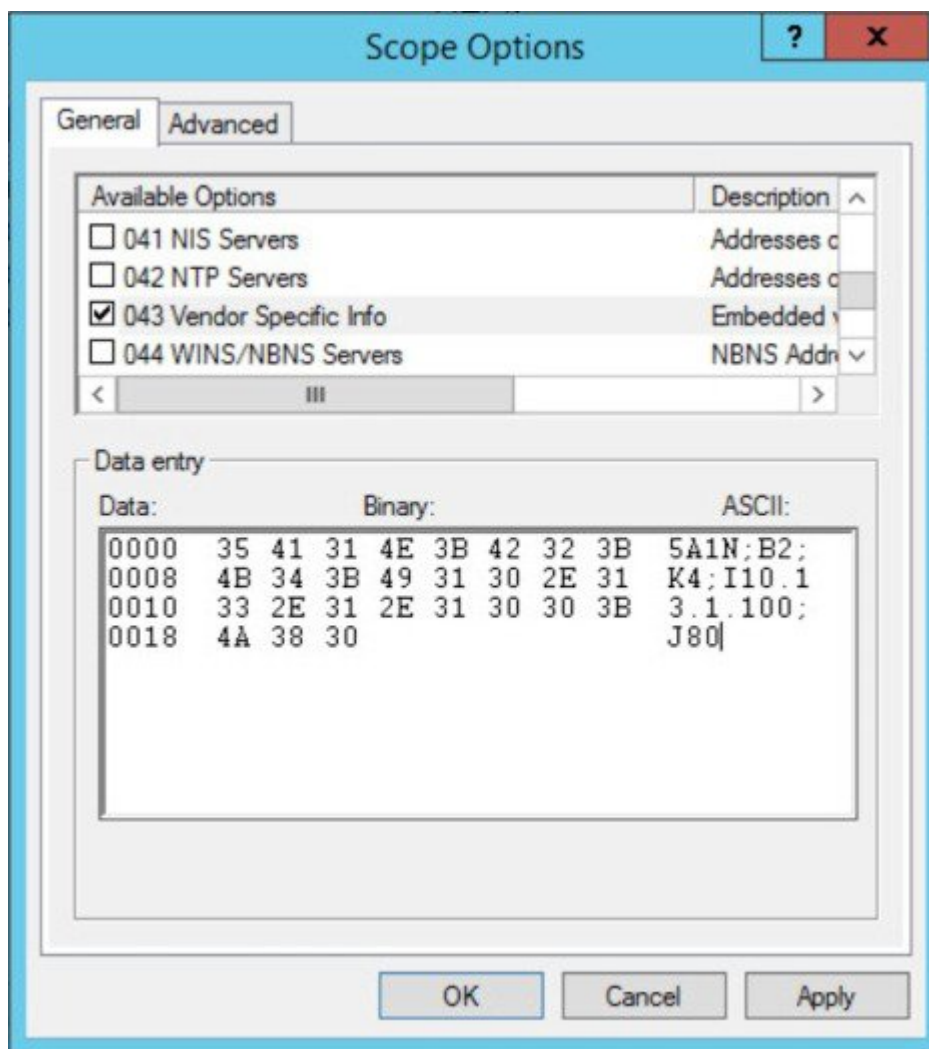
手順

ステップ 1 ホスト名が「PNPSEVER」、IP アドレスが PNP サーバの IP アドレスである DNS サーバ上でホストファイルを作成します。

ステップ2 DHCP スコープにオプション 15 を追加してドメイン名を入力し、オプション 6 に DNS サーバを追加します。

ステップ3 センサーの NTP サーバ IP アドレスをオプション 42 に追加できます。この DHCP オプション 42 の NTP サーバは、今後の AP1800s ソフトウェアのリリースには不要です。このオプションは、センサーの初回リリース 8.5.257 でのみ必要です。

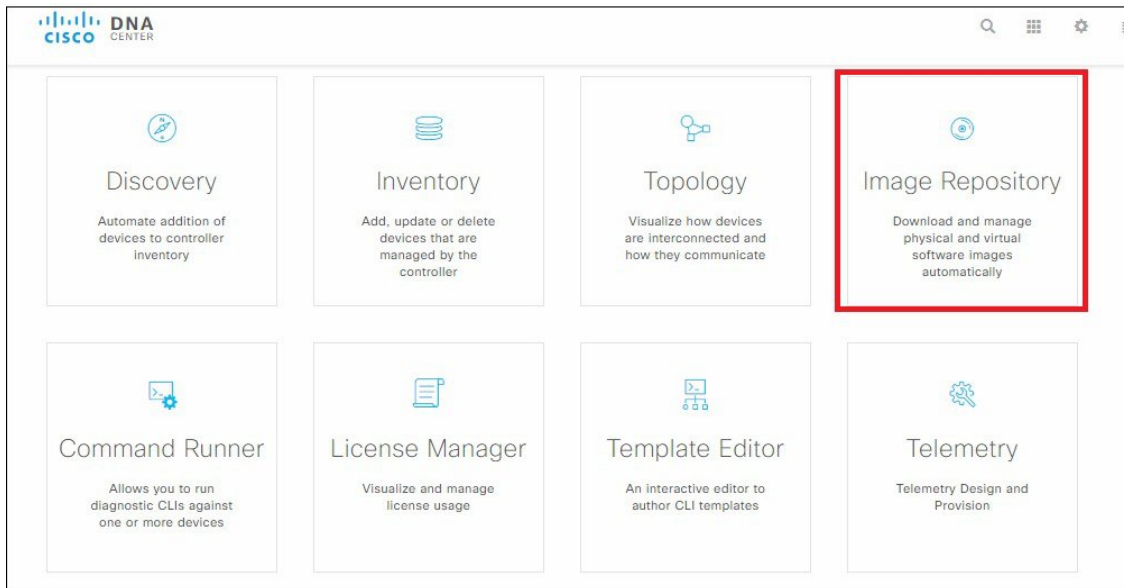
スコープ オプションの例：



オプション 43 および DNS の詳細については、次のガイドを参照してください。 https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#con_115699

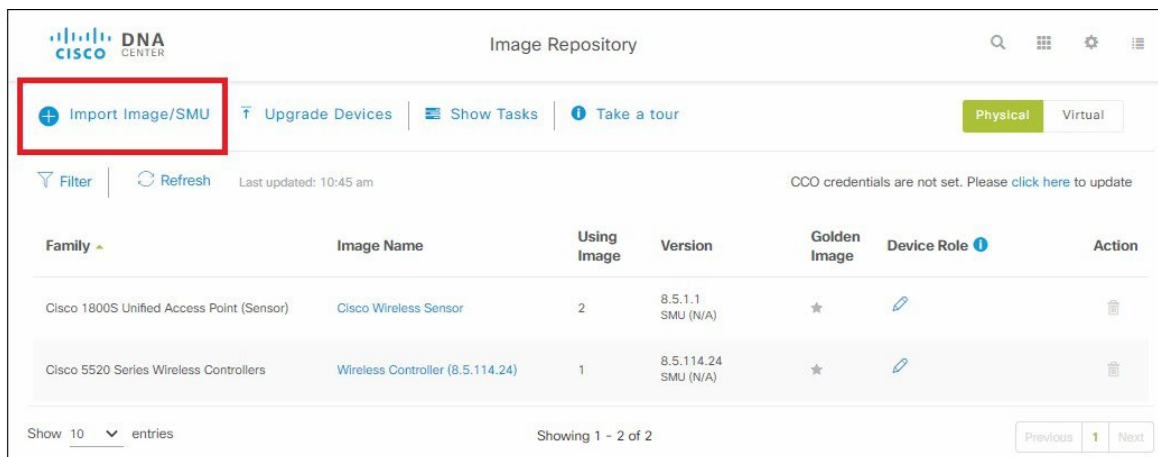
1852、2800、または 3800 センサーのイメージのアップグレードは、WLC 上のイメージをアップグレードすることによって行うことができます。

1800s のアップグレードは、DNAC を介して行うことができます。1800s を DNAC からアップグレードするには、初めにシスコの Web サイトからイメージをダウンロードして、次にそのイメージを DNAC のリポジトリに追加します。DNAC のメインページで一番下までスクロールして、イメージリポジトリをクリックします。



ステップ 4 DHCP オプション 43 フィールドを別の目的（AP のプロビジョニング用の WLC IP アドレスなど）ですで使用している場合、条件付きのオプション43フィールドをさらに追加することができます。これを行うには、条件付き割り当てとして VCI 文字列を追加します。シスコ アクティブセンサー AP1800s の VCI 文字列は、「Cisco AP C1800」です。

ステップ 5 [Import Image/SMU] をクリックします。



CCO からダウンロードした sn1g5-k9w8 イメージをインポートするか、URL を指定することで、イメージを追加できます。[Import (インポート)] ボタンをクリックします。

Import Image/SMU

Select a file from computer

[Choose File](#) sn1g5-k9w8-201801121543.tar.gz

OR

Enter Image URL(http or ftp)*

Source

Cisco Third Party

[Close](#) [Import](#)

これで、イメージがリポジトリに追加されます。「Cisco 1800S Unified Access Point (Sensor)」の横にある下矢印をクリックします。インポートされたイメージが一覧表示されます。インポート済みイメージの横にある、[Golden Image]列の星印をクリックします。これにより、リポジトリはセンサーにダウンロードするイメージを認識します。星印は、同時に1つのみ選択できます。

DNA CENTER
Image Repository
🔍 🏠 ⚙️ ☰

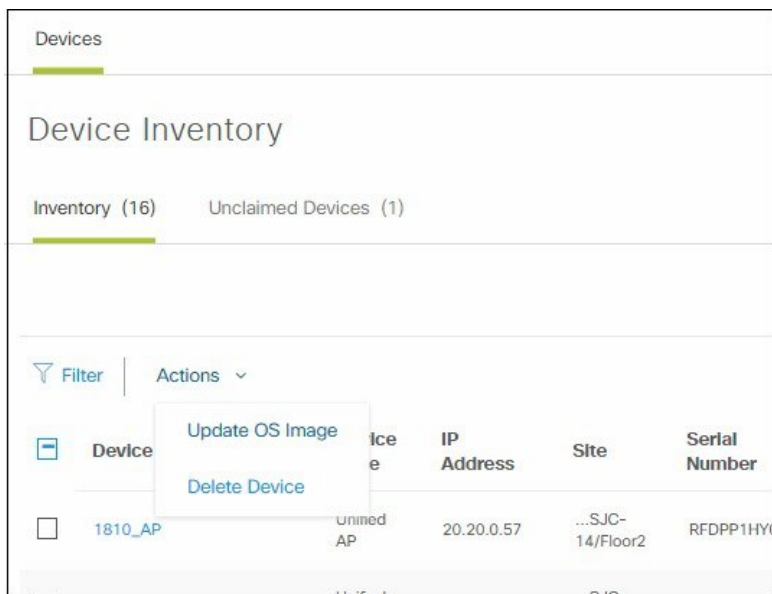
[+ Import Image/SMU](#)
[📄 Upgrade Devices](#)
[📋 Show Tasks](#)
[👤 Take a tour](#)
Physical
Virtual

🔽 Filter | 🔄 Refresh | Last updated: 10:50 am
CCO credentials are not set. Please [click here](#) to update

Family	Image Name	Using Image	Version	Golden Image	Device Role	Action
Cisco 1800S Unified Access Point (Sensor) ⌵	Cisco Wireless Sensor	2	8.5.1.1 SMU (N/A)	★	✎	🗑️
	sn1g5-k9w8-201801222254.tar... 🛑 Unable to verify	0	8.5.114.25 SMU (N/A)	★	✎ ALL ★	🗑️
Cisco 5520 Series Wireless Controllers	Wireless Controller (8.5.114.24)	1	8.5.114.24 SMU (N/A)	★	✎	🗑️

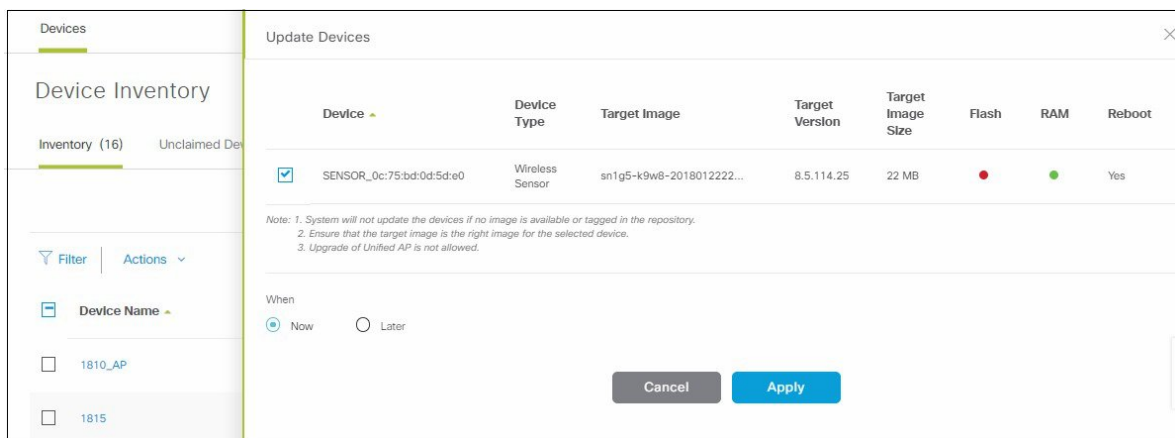
Show 10 entries
Showing 1 - 2 of 2
Previous
1
Next

[Upgrade Device] をクリックして、インベントリのページに移動します。アップグレードする 1800s を選択して、ページの上部の [Action] > [Update OS Image] を選択します。



新しいウィンドウが表示され、選択したセンサーとターゲットイメージがリストされます。

ステップ 6 [Now] または [Later] を選択して、アップグレードを実行します。



トラブルシューティング コマンド

トラブルシューティング用の CLI コマンドです。これらのコマンドは、センサー AP コンソール (telnet または ssh) から実行する必要があります。

```
# show dot11 sensor heartbeat status
```

DNAC とセンサー間のハートビートは、60 秒ごとに発生します。ハートビートのステータスと最後の成功時刻を表示するには、このコマンドを実行します。失敗している場合、DNAC への接続を確認します。

```
# show dot11 sensor test result
```

これは、センサーで実行されたテストの結果を示します。これらの結果は DNAC に直接送られ、WLC を経由しません。

```
# show dot11 sensor test config
```

これは、センサーが WLC を経由して DNAC から受信した構成を示します。

```
# show dot11 sensor synthetic work list
```

これは、センサーが実行する各テストの詳細を表示します。

```
# show dot11 sensor stats
```

実行したテスト ケースの合計、成功したテスト ケース、および失敗した テストースを調べます。これにより、センサーで実行されたテストの数、およびこれらのテストの状況の概要が表示されます。これには無線の統計情報も含まれ、DNAC 接続が有効かどうかを示されます。

```
# show dot11 sensor scan list
```

これは、センサーが受信できる AP および受信信号レベルを示します。RSSI が -75 以上の AP のみがテスト対象となります。

```
# debug wsa debug
```

wsa debug からの完全なデバッグ出力を表示するには、「term mon」を使用します。

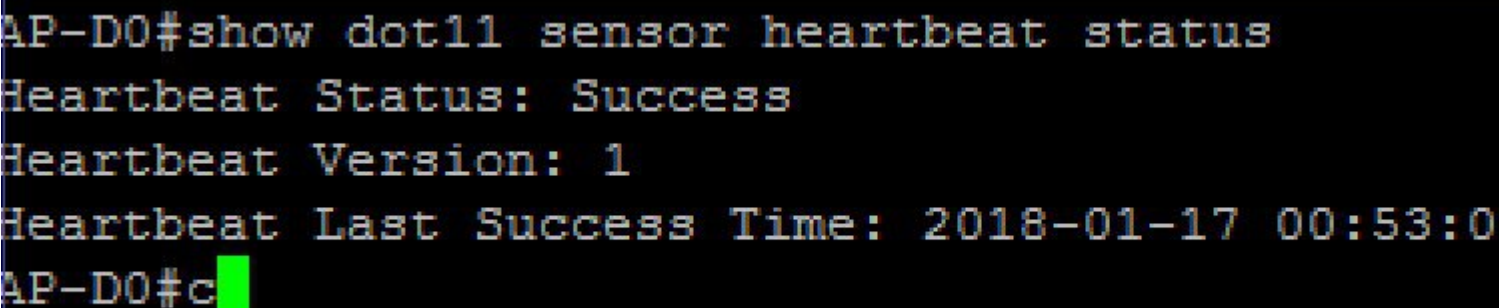
トラブルシューティング コマンド出力の詳細

```
STUB01-SENS3-1815I# show dot11 sensor heartbeat status
```

Heartbeat Status: Success

Heartback Version: 1

Heartbeat Last Success Time: 2018-01-17 00:53:08.016900



```
AP-D0#show dot11 sensor heartbeat status
Heartbeat Status: Success
Heartbeat Version: 1
Heartbeat Last Success Time: 2018-01-17 00:53:08.016900
AP-D0#c
```

```
STUB01-SENS3-1815I# show dot11 sensor test results
```

Test No: 1, Name: DNS, Time: 2018-01-09 18:48:17.464181

```
Test Results: {
  "macAddress": "00:a3:8e:16:05:a0",
  "testCompleted": "no",
  "type": "DEDICATED",
  "connectivityStats": {
    "wireless": {
      "status": "SUCCESS",
      "channelWidth": 20,
      "txDataRate": 24000,
      "responseTimesInMillis": {
```

```

        "probeRequest": 1,
        "authenticationRequest": 1,
        "handshake": 38,
        "associationRequest": 47
    },
    "snr": 60,
    "rssi": -35,
    "channel": 64
},
"DHCP": {
    "status": "SUCCESS",
    "totaltime": 4566,
    "slack": 0,
    "offer": 4202,
    "ack": 118,
    "IP": "10.40.233.115",
    "request": 30,
    "discover": 0,
    "DefaultGWIP": "10.40.239.254",
    "dhcpv6": 0,
    "DNSIP": "208.67.222.222",
    "FailureReason": "DHCP_SUCCESS"
},
"DefaultGW": {
    "reachabilityStatus": "yes",
    "reachabilityTimeMillis": "1.616"
},
"DNS-Server": {
    "reachabilityStatus": "yes",
    "reachabilityTimeMillis": "1.982"
}
}
<Remainder removed>

```

```

STUB01-SENS3-1815I#show dot11 sensor test results
Test No: 1, Name: DNS, Time: 2018-01-09 18:48:17.464181
Test Results: {
    "macAddress": "00:a3:8e:16:05:a0",
    "testCompleted": "no",
    "type": "DEDICATED",
    "connectivityStats": {
        "wireless": {
            "status": "SUCCESS",
            "channelWidth": 20,
            "txDataRate": 24000,
            "responseTimesInMillis": {
                "probeRequest": 1,
                "authenticationRequest": 1,
                "handshake": 38,
                "associationRequest": 47
            }
        },
        "snr": 60,
        "rssi": -35,
        "channel": 64
    }
},

```

```

STUB01-SENS3-1815I# show dot11 sensor test config
Test Config Received Time: 2018-01-09 05:57:18.971401
{
    advancedConfig: {
        rssiThreshold: -75
    }
}
testConfig:

```

```

{
  name: DNS
  bands: BOTH
  connection: WIRELESS
  frequency: {
    value: 30
    unit: MINUTES
  }
  ssids:
    {
      username: null
      validTo: 0
      numAps: 0
      id: 0
      authTypeRcvd: null
      authType: OTHER
      ssid: ubcvisitor
      authProtocol: null
      eapMethod: null
      certxferprotocol: HTTP
      status: ENABLED
      psk: null
      bands: 5GHz
      certfilename: null
      profileName: eduroam
      password: ****
      certstatus: ACTIVE
      wlc: 10.0.32.145
      certpassphrase: null
      numSensors: 0
      certdownloadurl: null
      wlanId: 0
      validFrom: 0
    }
}

```

```

STUB01-SENS3-1815I#show dot11 sensor test config
Test Config Received Time: 2018-01-09 05:57:18.971401
{
  advancedConfig: {
    rssiThreshold: -75
  }
  testConfig:
    {
      name: DNS
      bands: BOTH
      connection: WIRELESS
      frequency: {
        value: 30
        unit: MINUTES
      }
    }
  ssids:
    {
      username: null
      validTo: 0
      numAps: 0
      id: 0
      authTypeRcvd: null
      authType: OTHER
      ssid: ubcvisitor
    }
}

```

```

STUB01-SENS3-1815I# show dot11 sensor synthetic work list
Test 1 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 00:c8:8b:46:7b:ee radio 1

```

```

Wlan eduroam band 802.11a
ssid eduroam frequency 30 freq_unit MINUTES on_demand 0 repeatCountOnFailure 0

Test 2 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 1c:6a:7a:fc:0c:8e radio 1
Wlan eduroam band 802.11a
ssid eduroam frequency 30 freq_unit MINUTES on_demand 0 repeatCountOnFailure 0

Test 3 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 10:05:ca:72:06:de radio 1
Wlan eduroam band 802.11a
ssid eduroam frequency 30 freq_unit MINUTES on_demand 0 repeatCountOnFailure 0

Test 4 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 10:05:ca:c4:0b:7e radio 1
Wlan eduroam band 802.11a
ssid eduroam frequency 30 freq_unit MINUTES on_demand 0 repeatCountOnFailure 0

Test 5 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 1c:6a:7a:f2:0d:4e radio 1
Wlan eduroam band 802.11a
ssid eduroam frequency 30 freq_unit MINUTES on_demand 0 repeatCountOnFailure 0

Test 6 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 1c:6a:7a:fc:00:be radio 1
Wlan eduroam band 802.11a
ssid eduroam frequency 30 freq_unit MINUTES on_demand 0 repeatCountOnFailure 0

```

```

STUB01-SENS3-1815I#show dot11 sensor synthetic work list
Test 1 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 00:c8:8b:46:7b:ee radio 1 Wlan
Test 2 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 1c:6a:7a:fc:0c:8e radio 1 Wlan
Test 3 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 10:05:ca:72:06:de radio 1 Wlan
Test 4 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 10:05:ca:c4:0b:7e radio 1 Wlan
Test 5 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 1c:6a:7a:f2:0d:4e radio 1 Wlan
Test 6 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 1c:6a:7a:fc:00:be radio 1 Wlan
Test 7 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 1c:6a:7a:f2:1f:5e radio 1 Wlan
Test 8 Suite 5a331790d07f6f00201c8b0b_afdb243d-67bf-488b-a4d7-d8b59ae93868 DNS AP 10:05:ca:b4:81:8e radio 1 Wlan

```

```

STUB01-SENS3-1815I# show dot11 sensor stats
## Network Assurance Sensor Statistics ##
WSA Status: Enabled
NA Connectivity: Not Connected
NA Connectivity I/F: Radio 0 http
NA Server URL: https://10.0.32.42
Auth Type: 10
HTTP Proxy IP:
Backhaul SSID:
Id-token: <BASE64 Encoded String removed>
Port: 80
Total Test Cases Run: 0
Successful Test Cases: 0
Failed Test Cases: 0
Network Assurance 5G Radio Statistics
-----
Host Rx K Bytes: 58643
Host Tx K Bytes: 8097
Unicasts Rx: 267431
Unicasts Tx: 59926
Broadcasts Rx: 53327
Broadcasts Tx: 5550
Beacons Rx: 456662
Beacons Tx: 0
Multicasts Rx: 0
Multicasts Tx: 0
CRC errors: 4178

```

```

Network Assurance 2G Radio Statistics
-----

```


Host Rx K Bytes: 0

Sensor Troubleshooting on the WLC

Sensor Troubleshooting

- Confirm Sensor AP is in Sensor mode on the WLC
- Verify that all radio's are indeed up and operational

The screenshot shows the configuration page for a Sensor AP in Cisco DNA Center. The 'General' tab is selected. The 'AP Mode' dropdown menu is set to 'Sensor'. Below, the 'Radio Interfaces' section shows two radio interfaces (0 and 1) with 'Operational Status' 'UP' and 'Admin Status' 'Enable'.

Interface	Operational Status	Tx Unicast Packets	Rx Unicast Packets	Tx Non-Unicast Packets	Rx Non-Unicast Packets
0	UP	106865	1395326	0	0

Radio Slot#	Radio Interface Type	Module Type	Sub Band	Admin Status	Oper Status
0	802.11b/g/n	-	-	Enable	UP
1	802.11a/n/ac	-	-	Enable	UP

参考 URL

DNA Center に関するドキュメントを次に示します。

DNA Center 管理者ガイド :

http://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/admin/b_dnac_admin_guide_1_1.html

DNA センター インストール ガイド :

http://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/install/b_dnac_install_1_1_0.html

DNA Center のリリース ノート :

http://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-1/rn/b_dnac_release_notes_1_1.html

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0809R)

この資料の記載内容は2008年10月現在のものです。

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255 (フリーコール、携帯・PHS含む)

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>