

# Chromebook オンボーディング用の ISE 2.1 を設定する

## 目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[フローの概要](#)

[ネットワーク図](#)

[設定](#)

[MAB SSID への接続によるオンボーディング](#)

[Google 管理コンソールの設定](#)

[ISE 設定](#)

[コントローラの設定](#)

[Chromebook のオンボーディング](#)

[その他の使用例](#)

[PEAP SSID への接続によるオンボーディング](#)

[確認](#)

[トラブルシューティング](#)

[ISE でのデバッグ](#)

[Chromebook のログ](#)

[有用な Chromebook ブラウザ コマンド](#)

[よくある問題](#)

## 概要

このドキュメントでは、Chromebook のオンボーディングに対して Cisco Identity Service Engine (ISE) バージョン 2.1 およびワイヤレス LAN コントローラ (WLC) を設定する方法について説明します。

## 前提条件

### 要件

以下に関する基本的な知識があることが推奨されます。

- Cisco Identity Services Engine
- Google 管理コンソール
- Chromebook 用のドメイン登録ライセンスとデバイス ライセンスの購入およびインストール

### 使用するコンポーネント

- ISE 2.1
- WLC バージョン 8.0.133.0
- Chromebook (ドメイン登録ライセンスとデバイスライセンスを購入済み)

## フローの概要

フローは、Cisco Network Setup Assistant (NSA) をクライアントにプッシュする時期に応じて異なります。

**( ユーザがプロビジョニング SSID に接続する前に ) Cisco NSA がアウトオブバンドで拡張機能に追加された場合**

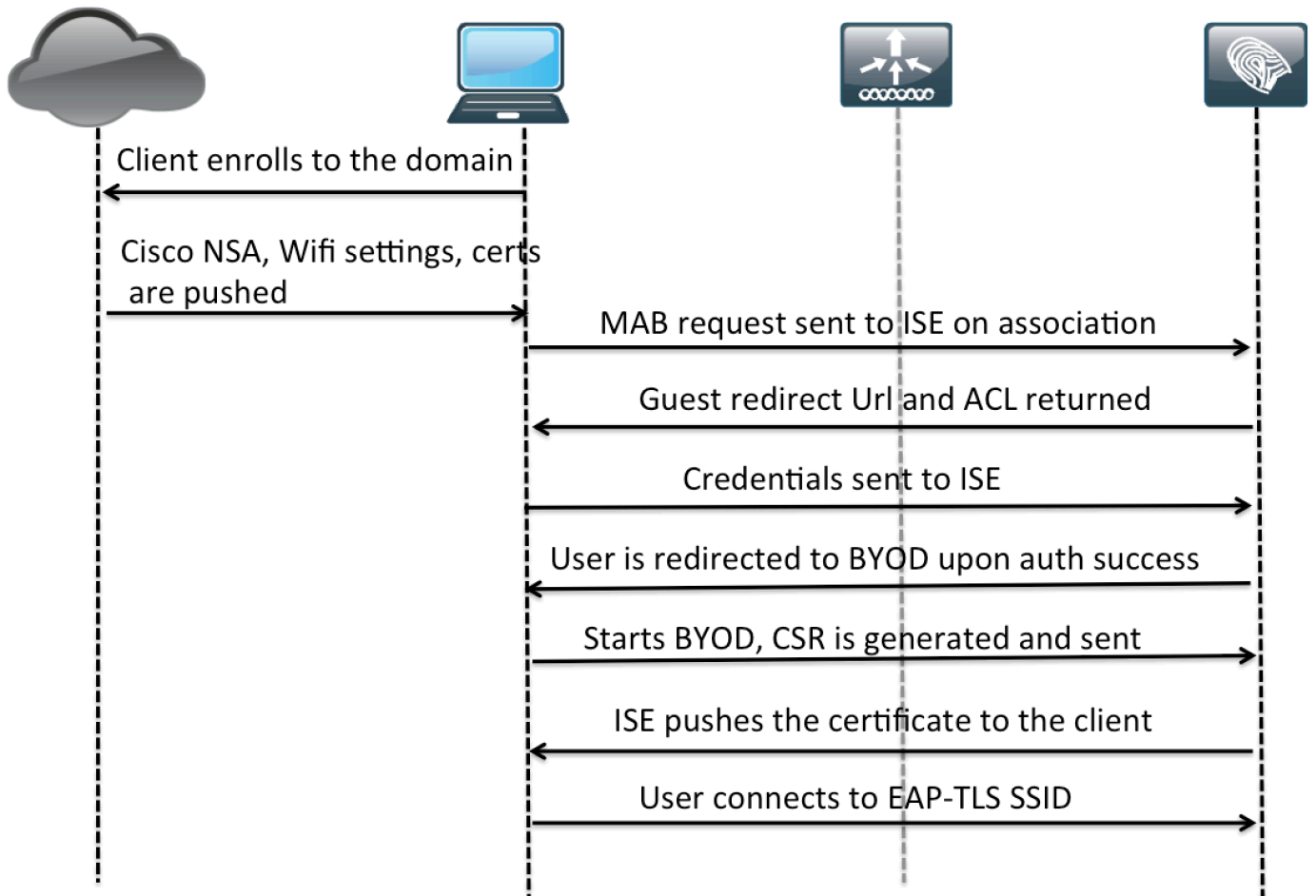
1. デバイスがドメインに登録され、Google 管理コンソールの設定に基づいて、Cisco NSA、WiFi 設定、証明書などが Chromebook によりダウンロードされます。
2. ユーザが MAB SSID に接続し、CWA にリダイレクトされます。
3. ユーザがクレデンシャルを入力します。認証に成功すると、ユーザは BYOD ポータルにリダイレクトされます。
4. BYOD が開始されると、クライアントによって CSR が ISE に送信されます。
5. ISE によって証明書が生成され、ユーザ証明書がクライアントにプッシュされます。
6. クライアントにプッシュされた証明書を使用して、Chromebook が TLS SSID に再接続されます。

**プロビジョニング SSID に接続した後に、Cisco NSA がダウンロードされた場合**

1. ユーザが MAB SSID に接続し、CWA にリダイレクトされます。リダイレクト ACL には、DNS、ISE、Google サーバ、Google ドメインへのアクセス権があります。
2. Google 管理コンソールで設定された Cisco NSA、WiFi 設定、証明書がデバイスによってダウンロードされます。
3. ユーザがゲスト ポータル ページでレデンシャルを入力します。認証に成功すると、ユーザは BYOD ポータルにリダイレクトされます。
4. BYOD が開始されると、クライアントによって CSR が ISE に送信されます。
5. ISE によって証明書が生成され、ユーザ証明書がクライアントにプッシュされます。
6. クライアントにプッシュされた証明書を使用して、Chromebook が TLS SSID に再接続されます。

## ネットワーク図

次のフローは、プロビジョニング SSID に接続する前に、Cisco NSA がエンドポイントに追加されるシナリオを示しています。



## 設定

### MAB SSID への接続によるオンボーディング

ユーザは MAB SSID に接続し、プロビジョニングされた証明書を取得して EAP-TLS に接続します。

#### Google 管理コンソールの設定

ステップ1: <https://admin.google.com> にアクセスして、Google 管理コンソールにログインします。

ステップ2: [Device management] > [Networks] > [Wifi] を参照して 2 つの WiFi 設定を追加します (一方はプロビジョニング SSID 用、もう一方は EAP-TLS 用)。

サーバ認証局: EAP-TLS WiFi の設定項目を設定する際に、EAP に内部 CA を使用している場合は、[Device Management] > [Network] > [Certificates] で、CA 証明書チェーンを管理コンソールにアップロードしなければなりません。アップロードした CA チェーンは、[Server Certificate Authority] でマッピングする必要があります。サードパーティの CA を使用している場合は、CA チェーンを管理コンソールにインポートする必要はなく、[Server Certificate Authority] のドロップダウンから [Use any default Certificate Authority] オプションを選択します。

発行者パターン/件名パターン: [Issuer Pattern] または [Subject Pattern] の 1 つ以上の属性が、インストールされている証明書の属性と一致しなければなりません。

## MAB SSID Wifi の設定 : Chrome-MAB

**Wi-Fi: Chrome-MAB**  
Locally applied [Help](#)

**Name**

**Service set identifier (SSID)**

This SSID is not broadcast  
 Automatically connect

**Security type**

**Proxy settings**

**Restrict access to this Wi-Fi network by platform**  
This Wi-Fi network will be available to users using:

- Mobile devices
- Chromebooks
- Chrome devices for meetings

**Apply network**  
by user (This setting cannot be changed in existing network)

## EAP-TLS SSID WiFi の設定 : Chrome-TLS

