Configurez ISE 2.1 pour Chromebook Onboarding

Contenu

Introduction

Ce document décrit comment configurer le contrôleur LAN de version 2.1 et de radio de l'engine de gestion d'identité de Cisco (ISE) (WLC) pour Chromebook onboarding.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de base du suivant

- Logiciel Cisco Identity Services Engine
- Console d'admin de Google
- En achetant et en installant l'enregistrement du domaine autorisez et permis de périphérique pour Chromebooks.

[Composants utilisés](#)

- ISE 2.1
- Version 8.0.133.0 WLC
- Chromebook (permis d'enregistrement du domaine et permis de périphérique acheté).

Aperçu d'écoulement

L'écoulement change selon quand la configuration réseau Assistant(NSA) de Cisco est poussée au client.

Si le NSA de Cisco est ajouté aux extensions hors de la bande (avant que l'utilisateur se connecte au ravitaillement SSID).

1. Le périphérique est enregistré au domaine et basé sur le config de la console d'admin de Google, Chromebook télécharge NSA de Cisco, configurations de WiFi, Certificats etc.

2. L'utilisateur se connecte au MAB SSID et obtient réorienté pour CWA.

3. L'utilisateur écrit des credentails. Sur l'authentification réussie, l'utilisateur est réorienté au portail BYOD.

4. Une fois que des débuts BYOD, CSR est envoyés à ISE par le client.

5. ISE génère le certificat et le certificat utilisateur est poussé au client.

6. Chromebook est rebranché au TLS SSID utilisant le certificat poussé au client.

Si le NSA de Cisco est téléchargé après s'être connecté au ravitaillement SSID.

1. L'utilisateur se connecte au MAB SSID et obtient réorienté pour CWA. Réorientez l'ACL a accès aux DN, ISE, serveurs de Google et domaine de Google.

2. Le périphérique télécharge le NSA de Cisco, des configurations de Wifi, des Certificats configurés sur la console d'admin de Google.

3. L'utilisateur écrit des credentails sur la page du portail d'invité. Sur l'authentification réussie, l'utilisateur est réorienté au portail BYOD.

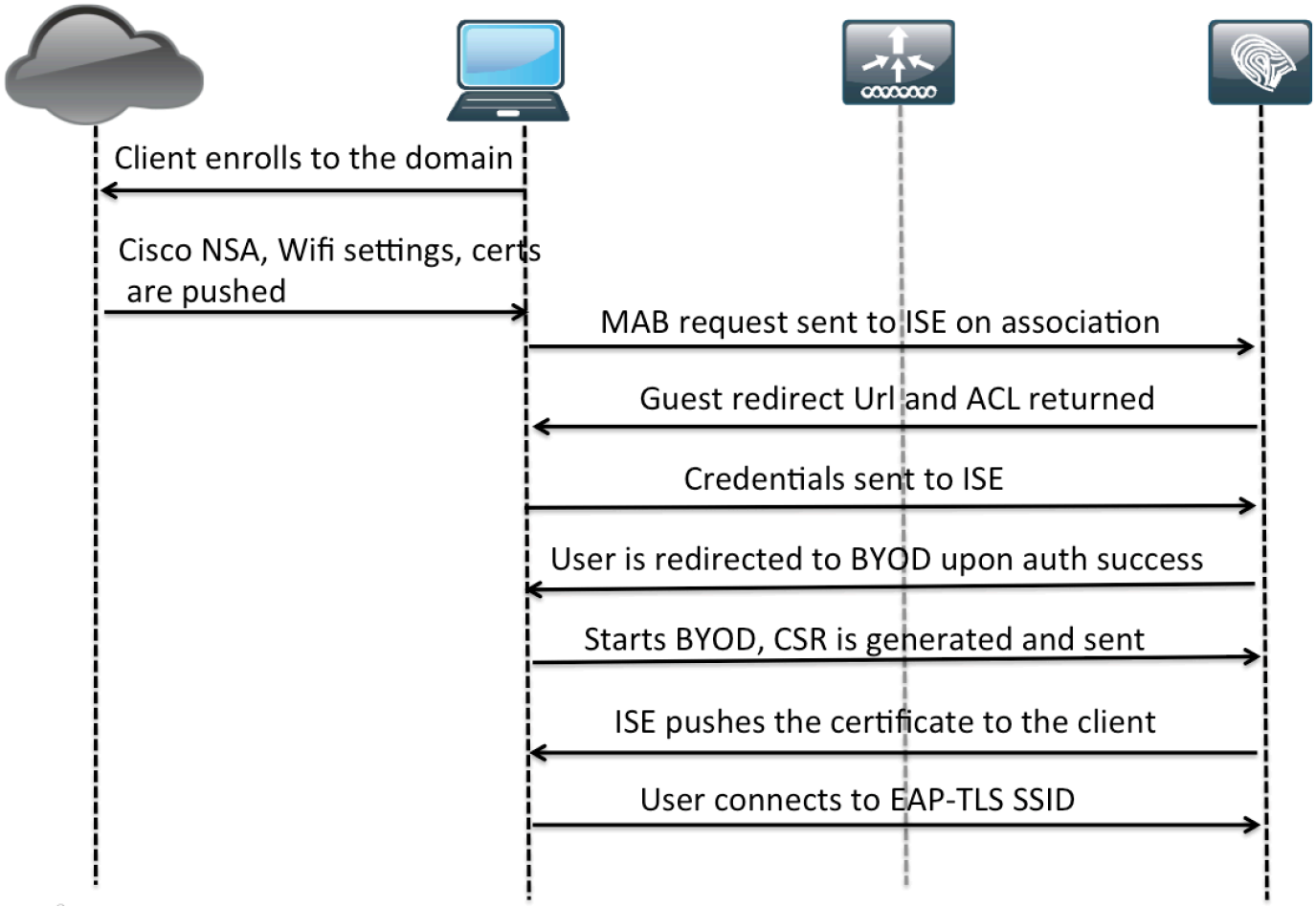
4. Une fois que des débuts BYOD, CSR est envoyés à ISE par le client.

5. ISE génère le certificat et le certificat utilisateur est poussé au client.

6. Chromebook est rebranché au TLS SSID utilisant le certificat poussé au client.

Diagramme du réseau

Cet écoulement décrit le scénario où le NSA de Cisco est ajouté au point final avant de se connecter au ravitaillement SSID.



Configurez

Onboarding en se connectant au MAB SSID

L'utilisateur se connecte au MAB SSID et obtient des Certificats provisioned pour se connecter à l'EAP-TLS.

Configuration de console d'admin de Google

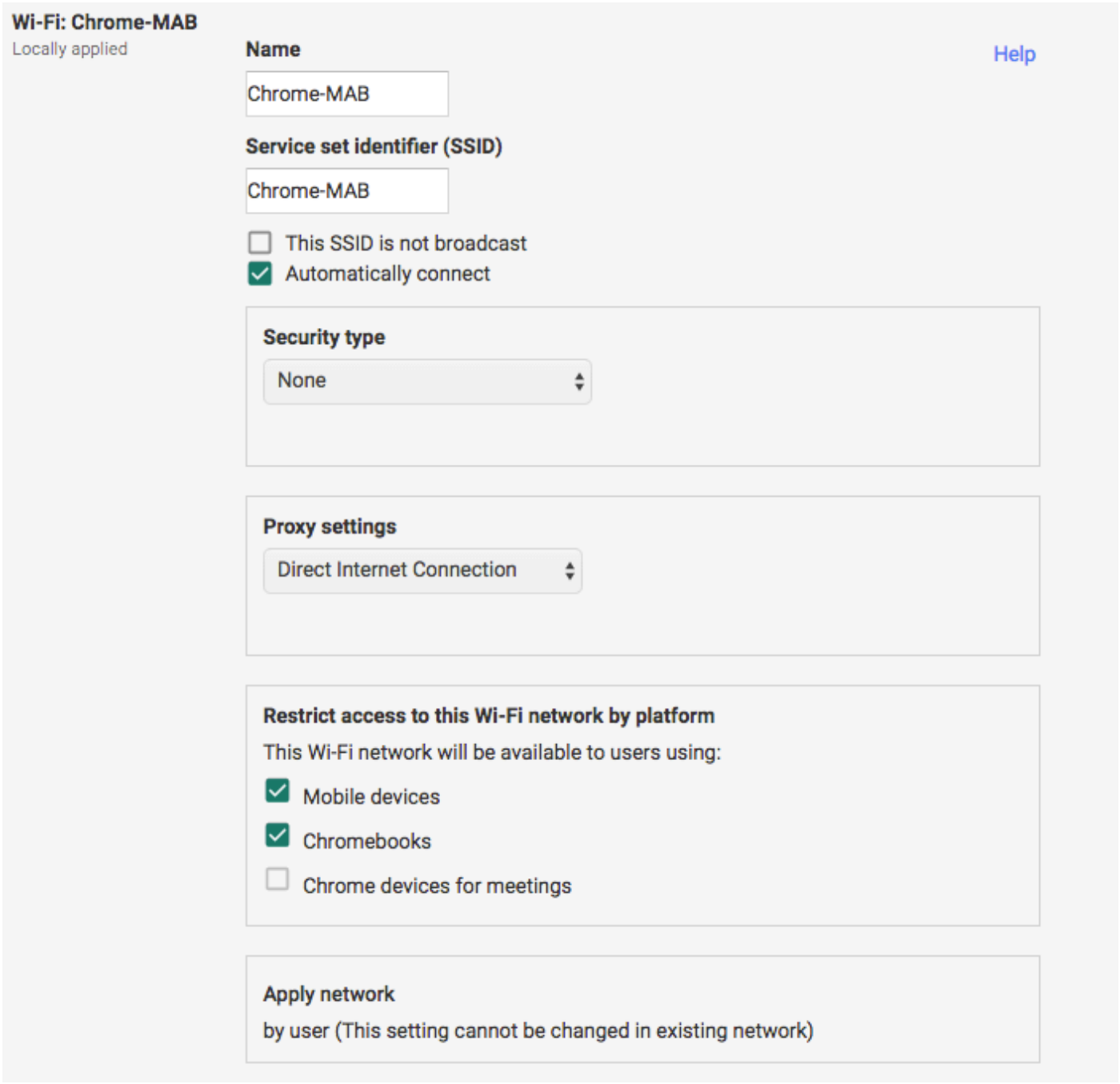
Step1 : Ouvrez une session à la console d'admin de Google en accédant à https://admin.Google.com

Step2 : Parcourez à la **Gestion de périphériques > aux réseaux > au Wifi** et ajoutez deux configurations de Wifi, une pour le ravitaillement SSID et autre pour l'EAP-TLS.

Autorité de certification de serveur : Tout en configurant des configurations de Wifi d'EAP-TLS, si vous utilisez un CA interne pour l'EAP, la chaîne de certificat de CA devrait être téléchargée à la console d'admin par l'intermédiaire de la **Gestion de périphériques > du réseau > des Certificats**. Une fois que la chaîne CA est téléchargée, elle doit être tracée sous l'autorité de certification de serveur. Si un tiers CA est utilisé, nous ne devons pas importer la chaîne CA à la console d'admin et sélectionner l'option « utilisation aucun Certificate Authority par défaut » de la baisse vers le bas de l'autorité de certification de serveur.

Modèle d'émetteur/modèle de sujet : Au moins un attribut de modèle d'émetteur ou de modèle soumis devrait apparier les attributs du certificat installé.

Configuration du MAB SSID Wifl : CHROME-MAB



Configuration de l'EAP-TLS SSID Wifi : CHROME-TLS