2.1 de la configuración ISE para Chromebook Onboarding

Contenido

Introducción

Este documento describe cómo configurar la versión 2.1 y el regulador del Wireless LAN (WLC) del motor del servicio de la identidad de Cisco (ISE) para Chromebook onboarding.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento básico del siguiente

- Cisco Identity Services Engine
- Consola de Google admin
- Comprando y instalando el registro de dominio autorice y licencia del dispositivo para Chromebooks.

Componentes Utilizados

- 2.1 ISE
- Versión 8.0.133.0 del WLC
- Chromebook (licencia del registro de dominio y licencia del dispositivo comprada).

Descripción del flujo

El flujo cambia dependiendo de cuando la configuración Assistant(NSA) de la red de Cisco se avanza al cliente.

Si Cisco NSA se agrega a las Extensiones fuera de la banda (antes de que el usuario conecta con la disposición del SSID).

1. El dispositivo se registra al dominio y basado en los config de la consola de Google admin, Chromebook descarga Cisco NSA, las configuraciones de WiFi, los Certificados etc.

2. El usuario conecta con el MAB SSID y consigue reorientado para CWA.

3. El usuario ingresa los credentails. Sobre la autenticación satisfactoria, reorientan al usuario al portal BYOD.

4. Una vez que BYOD comienza, el CSR es enviado al ISE por el cliente.

5. El ISE genera el certificado y el Certificado de usuario se avanza al cliente.

6. Chromebook se vuelve a conectar a TLS SSID usando el certificado avanzado al cliente.

Si Cisco NSA se descarga después de conectar con el SSID de disposición.

1. El usuario conecta con el MAB SSID y consigue reorientado para CWA. Reoriente el ACL tiene acceso al DNS, al ISE, a los servidores de Google y al dominio de Google.

2. El dispositivo descarga Cisco NSA, las configuraciones de Wifi, los Certificados configurados en la consola de Google admin.

3. El usuario ingresa los credentails en la página del portal del invitado. Sobre la autenticación satisfactoria, reorientan al usuario al portal BYOD.

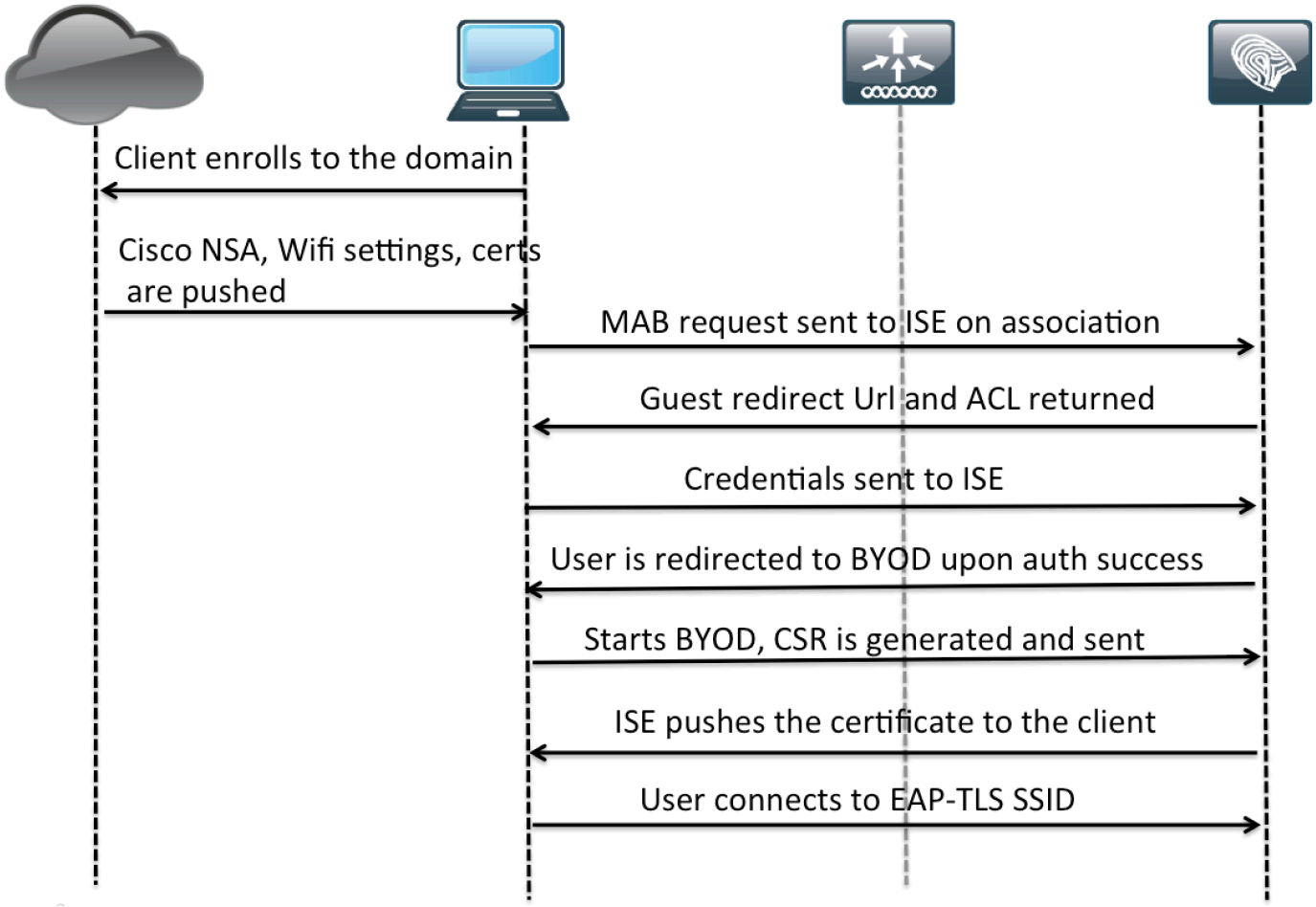
4. Una vez que BYOD comienza, el CSR es enviado al ISE por el cliente.

5. El ISE genera el certificado y el Certificado de usuario se avanza al cliente.

6. Chromebook se vuelve a conectar a TLS SSID usando el certificado avanzado al cliente.

Diagrama de la red

Este flujo describe el escenario donde Cisco NSA se agrega al punto final antes de conectar con la disposición del SSID.



Configurar

Onboarding conectando con MAB SSID

El usuario conecta con MAB SSID y consigue el aprovisionado de los Certificados para conectar con el EAP-TLS.

Configuración de la consola de Google Admin

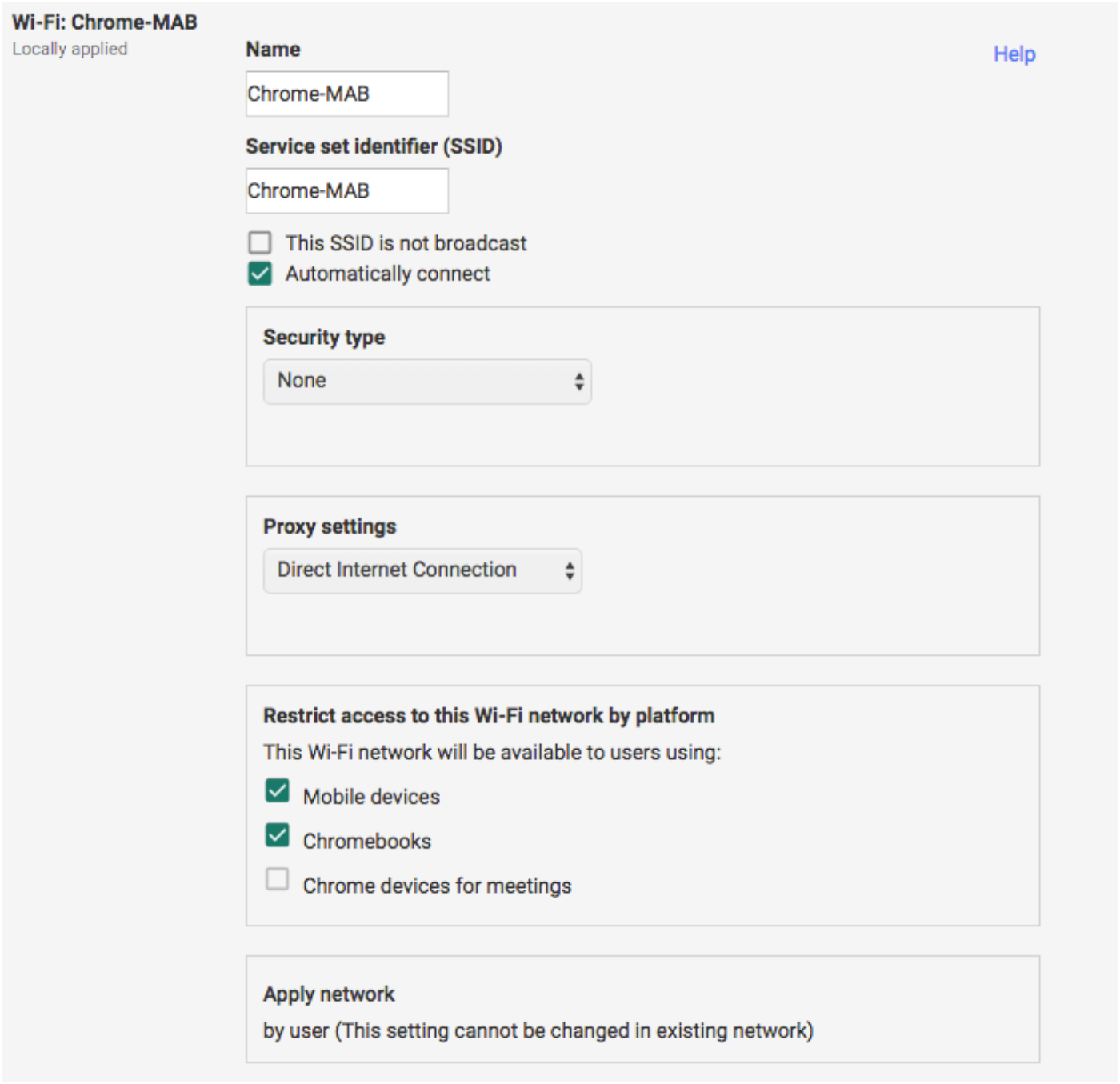
Step1: Login a la consola de Google admin accediendo https://admin.Google.com

Step2: Hojee a la **Administración de dispositivos > a las redes > a Wifi** y agregue dos configuraciones de Wifi, una para disposición el SSID y otra para el EAP-TLS.

Certificate Authority del servidor: Mientras que configura las configuraciones de Wifi del EAP-TLS, si usted está utilizando CA interno para el EAP, el encadenamiento del certificado de CA se debe cargar a la consola admin vía la **Administración de dispositivos > la red > los Certificados**. Una vez que el encadenamiento de CA está cargado, tiene que ser asociado bajo Certificate Authority del servidor. Si se está utilizando otro vendedor CA, no tenemos que importar el encadenamiento de CA a la consola admin y seleccionar la opción “uso ningún Certificate Authority predeterminado” del descenso abajo del Certificate Authority del servidor.

Modelo del emisor/modelo del tema: Por lo menos un atributo del modelo del emisor o del modelo del tema debe hacer juego los atributos del certificado instalado.

Configuración MAB SSID WifI: CHROME-MAB



Configuración del EAP-TLS SSID Wifi: CHROME-TLS