Configurar o 2.1 ISE para Chromebook Onboarding

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Vista geral do fluxo
Diagrama de Rede
Configurar
Onboarding conectando a MAB SSID
Configuração do console de Google Admin
Configuração ISE
Configuração de controle
Onboarding Chromebook
Caso adicional do uso
Onboarding conectando a PEAP SSID
Verificar
Troubleshooting
Debuga no ISE
Logs de Chromebook
Comandos úteis do navegador de Chromebook
Edições típicas

Introdução

Este documento descreve como configurar a versão 2.1 do motor do serviço da identidade de Cisco (ISE) e o controlador do Wireless LAN (WLC) para Chromebook que onboarding.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento básico do seguinte

- Cisco Identity Services Engine
- Console de Google admin
- Comprando e instalando o registro de domínio licencie e licença do dispositivo para Chromebooks.

Componentes Utilizados

- 2.1 ISE
- Versão 8.0.133.0 WLC
- Chromebook (licença do registro de domínio e licença do dispositivo comprada).

Vista geral do fluxo

O fluxo muda segundo quando a instalação Assistant(NSA) da rede Cisco é empurrada para o cliente.

Se Cisco NSA está adicionado aos Ramais fora da faixa (antes que o usuário conecta ao abastecimento SSID).

1. O dispositivo é registrado ao domínio e baseado na configuração do console de Google admin, das transferências Cisco NSA de Chromebook, dos ajustes de WiFi, dos Certificados etc.

2. O usuário conecta ao MAB SSID e obtém reorientado para CWA.

3. O usuário incorpora credentails. Em cima da autenticação bem sucedida, o usuário é reorientado ao portal BYOD.

4. Uma vez que BYOD começa, o CSR está enviado ao ISE pelo cliente.

5. O ISE gerencie o certificado e o certificado de usuário é empurrado para o cliente.

6. Chromebook é reconectado a TLS SSID usando o certificado empurrado para o cliente.

Se Cisco NSA é transferido após a conexão ao abastecimento SSID.

1. O usuário conecta ao MAB SSID e obtém reorientado para CWA. Reoriente o ACL tem o acesso ao DNS, ao ISE, aos server de Google e ao domínio de Google.

2. O dispositivo transfere Cisco NSA, ajustes de Wifi, os Certificados configurados no console de Google admin.

3. O usuário incorpora credentails na página do portal do convidado. Em cima da autenticação bem sucedida, o usuário é reorientado ao portal BYOD.

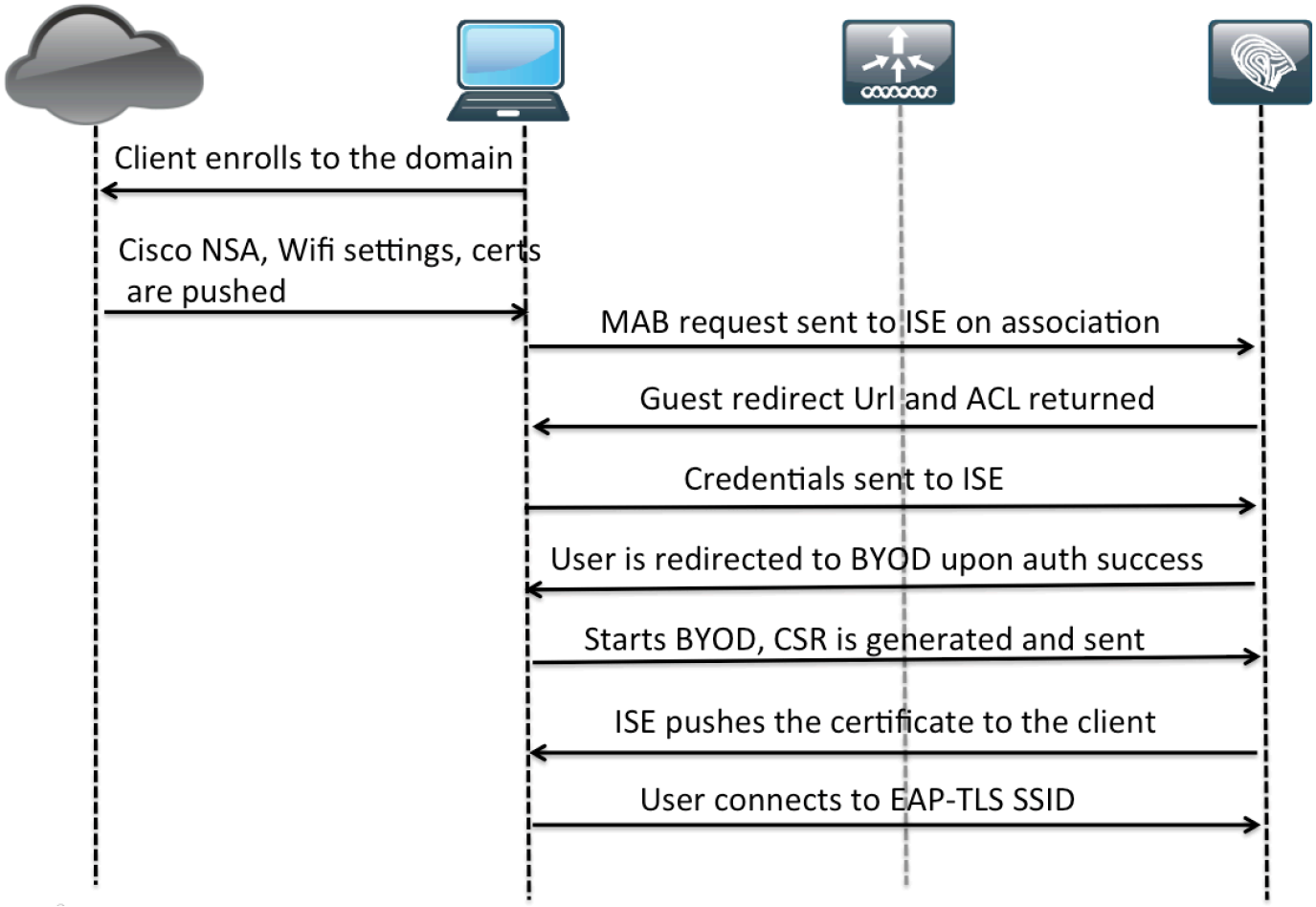
4. Uma vez que BYOD começa, o CSR está enviado ao ISE pelo cliente.

5. O ISE gerencie o certificado e o certificado de usuário é empurrado para o cliente.

6. Chromebook é reconectado a TLS SSID usando o certificado empurrado para o cliente.

Diagrama de Rede

Este fluxo descreve a encenação onde Cisco NSA é adicionado ao valor-limite antes de conectar ao abastecimento SSID.



Configurar

Onboarding conectando a MAB SSID

O usuário conecta com o MAB SSID e consegue Certificados fornecida conectar com o EAP-TLS.

Configuração do console de Google Admin

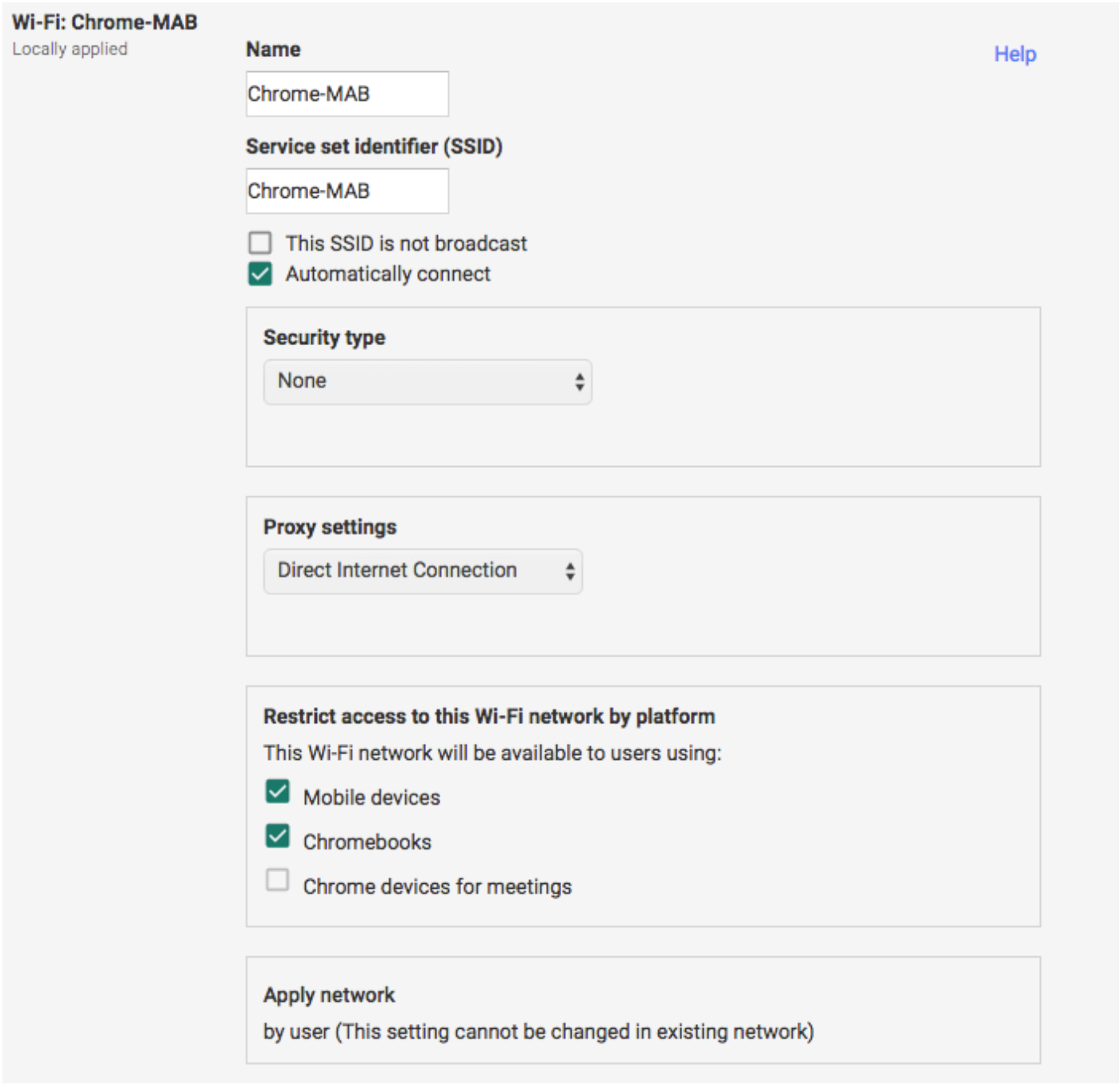
Step1: Início de uma sessão ao console de Google admin por https://admin.Google.com de acesso

Step2: Consulte ao **Gerenciamento de dispositivos > às redes > ao Wifi** e adicionar dois ajustes de Wifi, um para o abastecimento SSID e outro para o EAP-TLS.

Certificate Authority do server: Ao configurar ajustes de Wifi do EAP-TLS, se você está usando CA interno para o EAP, a corrente de certificado de CA deve ser transferida arquivos pela rede ao console admin através do **Gerenciamento de dispositivos > da rede > dos Certificados**. Uma vez que a corrente de CA é transferida arquivos pela rede, tem que ser traçada sob o Certificate Authority do server. Se uma terceira parte CA está sendo usada, nós não temos que importar a corrente de CA ao console admin e selecionar a opção “uso nenhum Certificate Authority do padrão” da gota para baixo do Certificate Authority do server.

Teste padrão do expedidor/teste padrão do assunto: Pelo menos um atributo do teste padrão do expedidor ou do teste padrão do assunto deve combinar os atributos do certificado instalado.

Ajuste MAB SSID WifI: Chrome-MAB



Ajuste do EAP-TLS SSID Wifi: Chrome-TLS