PORTAIL CAPTIF POUR LA SOCIETER JBT

Semih DAG

BTS SIO 2024-2025

Table des matières

1. Introduction

Dans le cadre de la sécurisation et de la gestion des accès Wi-Fi pour les visiteurs ou utilisateurs temporaires, la société JBT souhaite mettre en place un portail captif Cisco. Ce système permet d'intercepter les connexions Wi-Fi et de rediriger l'utilisateur vers une page d'authentification avant de lui accorder l'accès à Internet.

2. . Architecture nécessaire

- Cisco Wireless LAN Controller (WLC)
- Points d'accès Cisco compatibles
- Serveur DHCP pour fournir les IP
- Serveur Radius ou LDAP (optionnel pour authentification externe)
- Poste de gestion pour accéder à l'interface d'administration

3. . Configuration du WLAN invité

1. Accéder à l'interface Web du WLC :
2. Aller dans la section WLAN > Create New > Go
3. Nommer le WLAN : ex. 'WIFI_JBT_Invites'
4. Définir le SSID identique
5. Activer le WLAN à la fin de la configuration

4. Activer le portail captif (Web Auth)

1. Dans les paramètres du WLAN, aller dans Security > Layer 3
2. Activer Web Policy > Authentication
3. Choisir une méthode d'authentification : Local, Radius, LDAP
4. Sauvegarder la configuration

5. Mise en place d'une page d'accueil personnalisée

1. Dans la section Security > Web Auth > Web Login Page
2. Importer une page HTML personnalisée avec :
   - Logo JBT
   - Message de bienvenue
   - Zone de saisie pour login/mot de passe
3. Tester le rendu à l'aide d'un appareil connecté au SSID

6. Tests de fonctionnement

1. Connecter un terminal (PC, smartphone) au Wi-Fi invité
2. Vérifier la redirection automatique vers le portail captif

3. S’authentifier avec des identifiants valides
4. Vérifier l’accès Internet après authentification

7. Surveillance et suivi des connexions

1. Dans l’interface WLC, menu Monitor > Clients
2. Vérifier les sessions actives, les utilisateurs connectés
3. Exporter les journaux si nécessaire pour audit

8. Recommandations de sécurité

- Isoler le réseau invité du LAN principal (VLAN séparé)
- Limiter la durée d’accès (ex. 1h, 4h, 1 jour)
- Appliquer les règles de QoS pour éviter l’abus
- Utiliser HTTPS sur le portail pour la confidentialité des identifiants

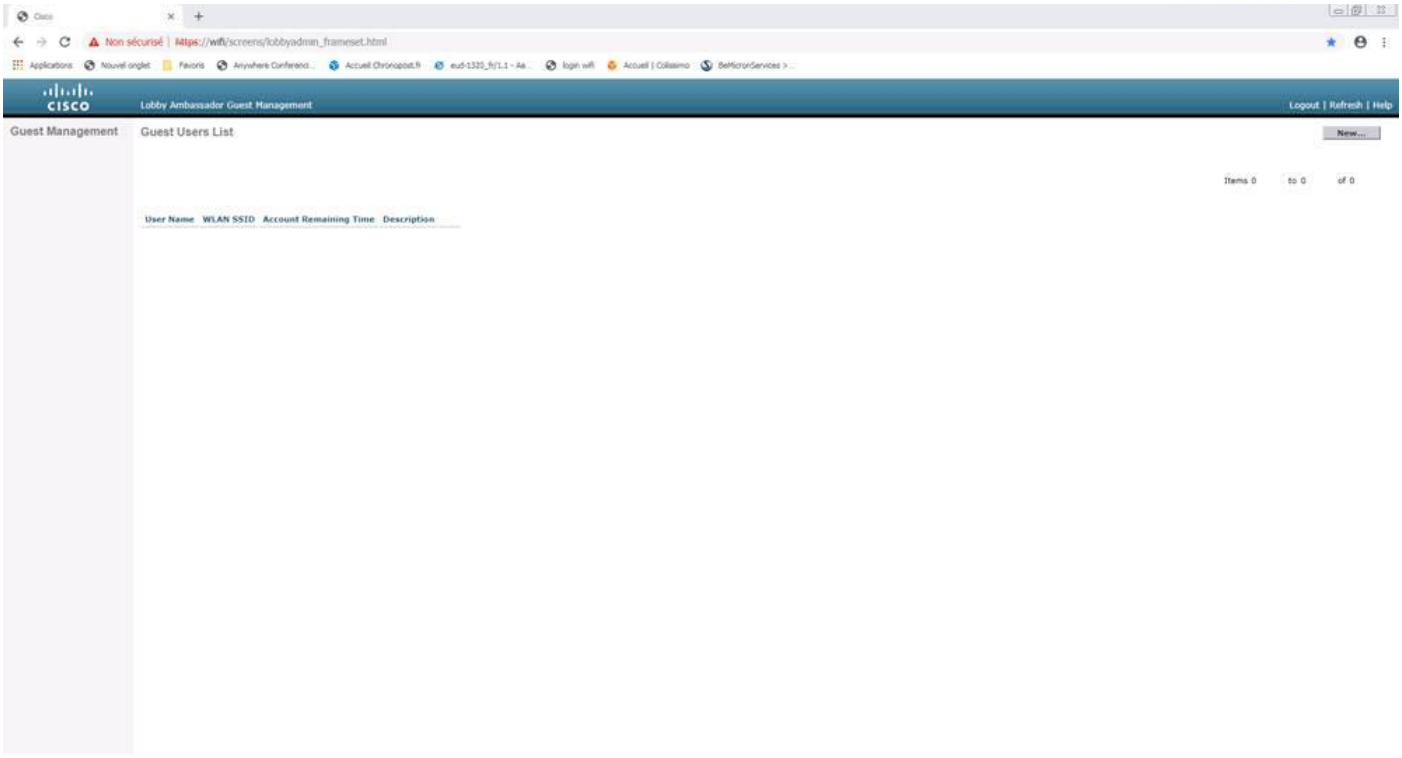
Étape 1- Accéder à l'interface de gestion
Ouvrir un navigateur Internet (Chrome, Firefox, Edge…).
Dans la barre d’adresse, saisir l’URL suivante :
https://10.68.1.51
Ce lien ne fonctionne qu’en interne, depuis le réseau de l’entreprise.

9. S’identifier sur le portail

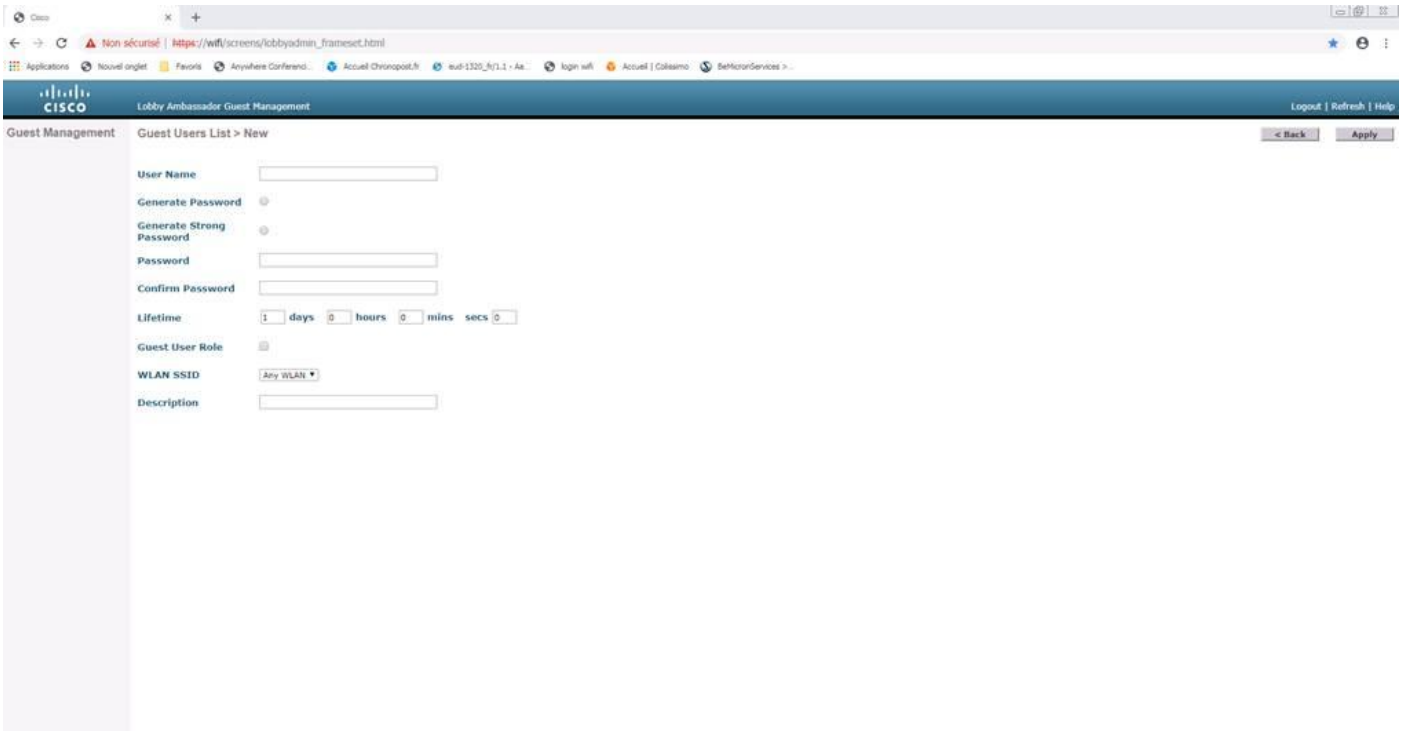
Une page d’authentification s’affiche.

ID : accueil
Mot de passe : jbMO2020*
Ces identifiants permettent d’accéder au panneau de création des comptes Wi-Fi .

1. Le portail ci-dessous :



2. Il faut sélectionner « NEW »



Créer un compte Wi-Fi visiteur
Une fois connecté, l'interface propose plusieurs options.

1. Cliquer sur le bouton **« NEW »** pour créer un nouvel accès.
2. Remplir les champs :
   Login : choisir un nom d'utilisateur (ex. : *visiteur123*)
   Mot de passe : créer un mot de passe temporaire
3. Définir la **durée d'utilisation** :
   Exemple : valable 1 jour, 3 heures, etc.
4. Dans la section **Type d'utilisateur**, sélectionner **« Externe »**.
5. Enfin, cliquer sur **« Apply »** pour valider la création du compte.

10. Communication aux visiteurs

Remettre au visiteur :

- Le **nom du réseau Wi-Fi**
- Le **login et mot de passe** créés
- Éventuellement, **une notice d'accès** s'il ne connaît pas le fonctionnement du portail captif.

Notes importantes

- Chaque visiteur doit avoir un **compte unique et temporaire**.
- La connexion est **filtrée et sécurisée**, conforme aux politiques internes de sécurité.
- Le compte peut être désactivé manuellement ou expirera automatiquement à la fin de la période définie.