Radio BYOD pour le guide de déploiement de FlexConnect

Contenu

Introduction

Les périphériques mobiles deviennent plus de calcul puissants et populaires parmi des consommateurs. Des millions de ces périphériques sont vendus aux consommateurs avec le WiFi ultra-rapide ainsi les utilisateurs peuvent communiquer et collaborer. Des consommateurs sont maintenant accoutumés à l'amélioration de la productivité que ces périphériques mobiles introduisent dans leurs vies et recherchent à introduire leur expérience personnelle dans l'espace de travail. Ceci crée les besoins de fonctionnalité d'une solution de Bring Your Own Device (BYOD) dans le lieu de travail.

Ce document fournit le déploiement de branchement pour la solution BYOD. Un employé se connecte à un Identifiant SSID (Service Set Identifier) entreprise à son nouvel iPad et obtient réorienté à un portail d'auto-enregistrement. Le Logiciel Cisco Identity Services Engine (ISE) authentifie l'utilisateur contre le Répertoire actif entreprise (AD) et télécharge un certificat avec une adresse MAC et un nom d'utilisateur inclus d'iPad à l'iPad, avec un profil de suppliant qui impose l'utilisation du Protocol-transport Layer Security (EAP-TLS) d'authentification extensible comme méthode pour la Connectivité de dot1x. Basé sur la stratégie d'autorisation dans ISE, l'utilisateur peut alors se connecter à l'utilisation du dot1x et accéder pour s'approprier des ressources.

Les fonctionnalités ISE dans des versions logicielles Sans fil de contrôleur LAN de Cisco plus tôt que 7.2.110.0 n'ont pas pris en charge les clients de commutation locale qui s'associent par les Points d'accès de FlexConnect (aps). La release 7.2.110.0 prend en charge ces fonctionnalités ISE pour FlexConnect aps pour la commutation locale et les clients centralement authentifiés. En outre, la release 7.2.110.0 intégré avec ISE 1.1.1 fournit (mais n'est pas limité à) ces caractéristiques de solution BYOD pour la radio :

- Profilage et posture de périphérique
- Enregistrement de périphérique et ravitaillement de suppliant
- Onboarding des périphériques personnels (IOS de disposition ou périphériques d'Android)

  Remarque: Bien que pris en charge, d'autres périphériques, tels que le PC ou les ordinateurs portables sans fil et les postes de travail de MAC, ne sont pas inclus dans ce guide.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Catalyst Switchs
- Contrôleurs Sans fil du RÉSEAU LOCAL de Cisco (WLAN)
- Version logicielle 7.2.110.0 du contrôleur de WLAN Cisco (WLC) et plus tard
- 802.11n aps en mode de FlexConnect
- Version de logiciel 1.1.1 et ultérieures de Cisco ISE
- AD de Windows 2008 avec l'Autorité de certification (CA)
- Serveur DHCP
- Serveur de Système de noms de domaine (DNS)
- Protocole NTP (Network Time Protocol)
- Ordinateur portable, smartphone, et tablettes de client sans fil (IOS d'Apple, Android, Windows, et MAC)

Remarque: Référez-vous aux notes de mise à jour pour les contrôleurs LAN Sans fil et le Point d'accès léger de Cisco pour la release 7.2.110.0 pour les informations importantes au sujet de cette version logicielle. Ouvrez une session au site de Cisco.com pour les dernières notes de mise à jour avant que vous chargiez et testiez le logiciel.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Topologie

Une configuration réseau minimale, suivant les indications de ce diagramme est exigée afin de correctement implémenter et tester ces caractéristiques :

Pour cette simulation, vous avez besoin d'un réseau avec un FlexConnect AP, des gens du pays/site distant avec le DHCP de gens du pays, DN, le WLC, et l'ISE. Le FlexConnect AP est connecté à un joncteur réseau afin de tester la commutation locale avec des VLAN multiples.

Enregistrement de périphérique et ravitaillement de suppliant

Un périphérique doit être enregistré de sorte que son suppliant indigène puisse provisioned pour l'authentification de dot1x. Basé sur la bonne stratégie d'authentification, l'utilisateur est réorienté à la page d'invité et authentifié par des qualifications des employés. L'utilisateur voit la page d'inscription de périphérique, qui demande leur information sur le périphérique. Le processus d'approvisionnement de périphérique commence alors. Si le système d'exploitation (SYSTÈME D'EXPLOITATION) n'est pas pris en charge pour le ravitaillement, l'utilisateur est réorienté au portail d'enregistrement de ressource afin de marquer que périphérique pour l'accès de dérivation d'authentification MAC (MAB). Si le SYSTÈME D'EXPLOITATION est pris en charge, le procédé d'inscription commence et configure le suppliant indigène du périphérique pour l'authentification de dot1x.

Portail d'enregistrement de ressource

Le portail d'enregistrement de ressource est l'élément de la plate-forme ISE qui permet à des employés pour initier onboarding des points finaux par une authentification et une procédure d'enregistrement.

Les administrateurs peuvent supprimer des ressources de la page d'identités de points finaux. Chaque employé peut éditer, supprimer, et mettre les ressources qu'sur la liste noireelles se sont enregistrées. Des points finaux mis sur la liste noire sont assignés à un groupe d'identité de liste noire, et une stratégie d'autorisation est créée afin d'empêcher l'accès au réseau par des points finaux mis sur la liste noire.

Portail d'Auto-enregistrement

Dans l'écoulement central de l'authentification Web (CWA), des employés sont réorientés à un portail qui leur permet pour entrer dans leurs qualifications, pour authentifier, et écrire les particularités de la ressource particulière qu'elles souhaitent s'enregistrer. Ce portail s'appelle le ravitaillement d'individu portail et est semblable au portail d'enregistrement de périphérique. Il permet aux employés pour entrer dans l'adresse MAC aussi bien qu'un escription signicatif du point final.

Authentification et ravitaillement

Une fois que les employés sélectionnent le portail d'Auto-enregistrement, ils sont défiés de fournir un ensemble de qualifications valides des employés afin de poursuivre à la phase de ravitaillement. Après l'authentification réussie, le point final peut provisioned dans la base de données de points finaux, et un certificat est généré pour le point final. Un lien à la page permet à l'employé pour télécharger l'assistant de pilote de suppliant (SPW).

> Remarque: Référez-vous à l'article de Cisco de matrice de caractéristique de FlexConnect afin de visualiser la dernière matrice de caractéristique de FlexConnect pour BYOD.

Ravitaillement pour IOS (iPhone/iPad/iPod)

Pour la configuration d'EAP-TLS, ISE suit Apple au-dessus de - aérez le procédé de l'inscription (OTA) :

- Après l'authentification réussie, l'engine d'évaluation évalue des stratégies de client-ravitaillement, qui a comme conséquence un profil de suppliant.
- Si le profil de suppliant est pour la configuration d'EAP-TLS, le processus OTA détermine si l'ISE est utilisation auto-signée ou signée par un CA inconnu. Si une des conditions est vraie, l'utilisateur est invité à télécharger le certificat d'ISE ou de CA avant que le procédé d'inscription puisse commencer.
- Pour d'autres méthodes d'EAP, ISE pousse le profil final sur l'authentification réussie.

Ravitaillement pour Android

En raison des considérations liées à la sécurité, l'agent d'Android doit être téléchargé du site de marché d'Android et ne peut pas provisioned d'ISE. Cisco télécharge une version de candidat de release de l'assistant dans le marché d'Android par le compte d'éditeur de marché de Cisco Android.

C'est le processus d'approvisionnement d'Android :

1. Cisco emploie le kit de développement logiciel (SDK) afin de créer le module d'Android avec une extension .apk.
2. Cisco télécharge un module dans le marché d'Android.
3. L'utilisateur configure la stratégie dans le ravitaillement de client avec les paramètres appropriés.
4. Après enregistrement du périphérique, l'utilisateur final est réorienté au service de

ravitaillement de client quand l'authentification de dot1x échoue.
5. La page du portail de ravitaillement fournit un bouton qui réoriente l'utilisateur au portail de marché d'Android où ils peuvent télécharger le SPW.
6. Cisco SPW est lancé et effectue le ravitaillement du suppliant : SPW découvre l'ISE et télécharge le profil d'ISE.SPW crée un CERT/paire de clés pour l'EAP-TLS.SPW fait un appel simple de demande de proxy de Protocol d'inscription de certificat (SCEP) à ISE et obtient le certificat.SPW applique les profils Sans fil.SPW déclenche la ré-authentification si les profils sont appliqués avec succès.Sorties SPW.

Double Auto-enregistrement Sans fil SSID BYOD

C'est le procédé pour le double auto-enregistrement Sans fil SSID BYOD :

1. Les associés d'utilisateur à l'invité SSID.
2. L'utilisateur ouvre un navigateur et est réorienté au portail d'invité ISE CWA.
3. L'utilisateur écrit un nom d'utilisateur et mot de passe des employés dans le portail d'invité.
4. ISE authentifie l'utilisateur, et, basé sur le fait qu'ils sont un employé et pas un invité, réoriente l'utilisateur à la page d'invité d'enregistrement de périphérique des employés.
5. L'adresse MAC pré-est remplie dans la page d'invité d'enregistrement de périphérique pour le DeviceID. L'utilisateur écrit une description et reçoit la Politique d'Utilisation Acceptable (AUP) s'il y a lieu.
6. L'utilisateur sélectionne **reçoivent** et commencent à télécharger et installer le SPW.
7. Le suppliant pour le périphérique de cet utilisateur provisioned avec tous les Certificats.
8. Le CoA se produit, et le périphérique rassocie au SSID entreprise (Corp.) et authentifie avec l'EAP-TLS (ou toute autre authorization method en service pour ce suppliant).

Auto-enregistrement Sans fil simple SSID BYOD

Dans ce scénario, il y a un SSID simple pour l'accès d'entreprise (Corp.) ce Protected Extensible Authentication Protocol de supports (PEAP) et EAP-TLS. Il n'y a aucun invité SSID.

C'est le procédé pour l'auto-enregistrement Sans fil simple SSID BYOD :

1. Les associés d'utilisateur à la corp.
2. L'utilisateur écrit un nom d'utilisateur et mot de passe des employés dans le suppliant pour l'authentification PEAP.
3. L'ISE authentifie l'utilisateur, et, basé sur la méthode PEAP, fournit une stratégie d'autorisation de reçoit avec le redirect to la page d'invité d'enregistrement de périphérique des employés.
4. L'utilisateur ouvre un navigateur et est réorienté à la page d'invité d'enregistrement de périphérique des employés.
5. L'adresse MAC pré-est remplie dans la page d'invité d'enregistrement de périphérique pour le DeviceID. L'utilisateur écrit une description et reçoit l'AUP.
6. L'utilisateur sélectionne **reçoivent** et commencent à télécharger et installer le SPW.
7. Le suppliant pour le périphérique de cet utilisateur provisioned avec tous les Certificats.
8. Le CoA se produit, et le périphérique rassocie à la Corp. SSID et authentifie avec l'EAP-TLS.

Configuration de caractéristique

Terminez-vous ces étapes afin de commencer la configuration :

1. Pour ce guide, assurez-vous que la version WLC est 7.2.110.0 ou plus tard.

2. Naviguez vers le **Security > Radius > Authentication**, et ajoutez le serveur de RAYON au WLC.

3. Ajoutez l'ISE 1.1.1 au WLC :

   Écrivez un secret partagé.Placez le soutien de RFC 3576 à **activer**.

4. Ajoutez le même serveur ISE qu'un serveur de comptabilité de RAYON.

5. Créez un ACL WLC Pre-Auth pour l'utiliser dans la stratégie ISE plus tard. Naviguez vers **WLC > Sécurité > listes de contrôle d'accès > FlexConnect ACLs**, et créez un nouvel ACL de FlexConnect nommé **ACL-REDIRECT** (dans cet exemple).

6. Dans les règles d'ACL, permettez tout le trafic à/de l'ISE, et permettez le trafic de client pendant le ravitaillement de suppliant.

   Pour la première règle (ordre 1) :

   En placez la source à.Place IP () d'adresse ISE/netmask **255.255.255.255**.Placez l'action **de laisser**.

   Pour deuxième règle (ordre 2), place source ip () d'adresse ISE/masque 255.255.255.255 à **quels** et action **de laisser**.

7. Créez un nouveau groupe de FlexConnect nommé Flex1 (dans cet exemple) :

   Naviguez vers l'onglet de **groupe >** de **WebPolicies de FlexConnect**.Sous le champ d'ACL de WebPolicy, cliquez sur Add, et sélectionnez **ACL-REDIRECT** ou l'ACL de FlexConnect créé

précédemment.Confirmez qu'il remplit champ de **listes de contrôle d'accès de WebPolicy**.

8. Cliquez sur Apply et **save configuration**.

Configuration WLAN

Terminez-vous ces étapes afin de configurer le WLAN :

1. Créez un WLAN ouvert SSID pour le double exemple SSID :

   Écrivez un nom WLAN : **DemoCWA** (dans cet exemple).Sélectionnez l'option **activée** pour l'état.

2. Naviguez vers l'onglet d'**onglet Sécurité >** de **couche 2**, et placez ces attributs :

   Degré de sécurité de la couche 2 : **Aucun**Filtrage MAC : **Activé** (la case est cochée)Transition rapide : **Handicapé** (la case n'est pas cochée)

3. Allez à l'**onglet AAA Servers**, et placez ces attributs :

   Serveurs d'authentification et de compte : **Activé**Serveur 1 : *Adresse IP <ISE >*

4. Faites descendre l'écran de l'**onglet AAA Servers**. Sous la commande d'authentication priority pour l'utilisateur de Web-auth, assurez-vous que le **RAYON** est utilisé pour l'authentification et les autres ne sont pas utilisés.

5. Allez à l'**onglet Avancé**, et placez ces attributs :

   Allow AAA Override : **Activé**État NAC : **Rayon NAC**
   Remarque: Le Contrôle d'admission au réseau (NAC) de RAYON n'est pas pris en charge quand le FlexConnect AP est dans le mode déconnecté. Ainsi, si le FlexConnect AP est en mode autonome et perd la connexion au WLC, tous les clients sont déconnectés, et le SSID n'est plus annoncé.
6. Faites descendre l'écran dans l'onglet Avancé, et placez la commutation locale de FlexConnect à **activer**.

7. Cliquez sur Apply et **save configuration**.

8. Créez un 802.1X WLAN SSID nommé **Demo1x** (dans cet exemple) pour les scénarios simples et doubles SSID.

9. Naviguez vers l'onglet d'**onglet Sécurité** > de **couche 2**, et placez ces attributs :

   Degré de sécurité de la couche 2 : **WPA+WPA2**Transition rapide : **Handicapé** (la case n'est pas cochée)Gestion des clés d'authentification : 802.IX : **Enable**

10. Allez à l'**onglet Avancé**, et placez ces attributs :

    Allow AAA Override : **Activé**État NAC : **Rayon NAC**

11. Faites descendre l'écran dans l'**onglet Avancé**, et placez la commutation locale de FlexConnect à **activer**.

12. Cliquez sur Apply et **save configuration**.

13. Confirmez que chacun des deux nouveaux WLAN ont été créés.

Configuration de FlexConnect AP

Terminez-vous ces étapes afin de configurer le FlexConnect AP :

1. Naviguez vers **WLC > radio**, et cliquez sur la cible FlexConnect AP.

2. Cliquez sur l'onglet de **FlexConnect**.

3. Le support de l'enable VLAN (la case est cochée), a placé l'ID DE VLAN indigène, et des **mappages du** clic **VLAN**.

4. Placez l'ID DE VLAN à **21** (dans cet exemple) pour le SSID pour la commutation locale.

5. Cliquez sur Apply et **save configuration**.

Configuration ISE

Terminez-vous ces étapes afin de configurer l'ISE :

1. Procédure de connexion au serveur ISE : < *https://ise* >.

2. Naviguez vers la **gestion** > la **Gestion de l'identité** > des **sources extérieures d'identité**.

3. **Répertoire actif de** clic.

4. Dans l'onglet Connection :

   Ajoutez le nom de domaine de **corp.rf-demo.com** (dans cet exemple), et changez le par défaut de nom de mémoire d'identité à **AD1**.**Save configuration de** clic.Cliquez sur **joignent**, et fournissent le nom d'utilisateur et mot de passe de compte administrateur d'AD requis se joindre.L'état doit être vert. Enable **connecté à :** (la case est cochée).

5. Réalisez un essai de base de connexion à l'AD avec un utilisateur en cours de domaine.

6. Si la connexion à l'AD est réussie, un dialogue confirme que le mot de passe est correct.

7. Naviguez vers la **gestion** > la **Gestion de l'identité** > des **sources extérieures d'identité** :

   Profil d'authentification de certificat de clic.Cliquez sur Add pour un nouveau profil d'authentification de certificat (CAP).

8. Écrivez un nom de **CertAuth** (dans cet exemple) pour la CAP ; pour l'attribut du nom d'utilisateur X509 de principal, **nom commun** choisi ; puis, cliquez sur Submit.

9. Confirmez que la nouvelle CAP est ajoutée.

10. Naviguez vers des **ordres de source de gestion >** de **Gestion de l'identité >** d'**identité**, et cliquez sur Add.

11. Donnez à l'ordre un nom de **TestSequence** (dans cet exemple).

12. Faites descendre l'écran **pour délivrer un certificat l'authentification basée** :

    Profil choisi d'authentification de certificat d'enable (la case est cochée).**Un CertAuth** choisi (ou un profil différent de CAP créé plus tôt).

13. Faites descendre l'écran à la **liste de recherche d'authentification** :

    Déplacez AD1 de disponible à sélectionné.Cliquez sur le bouton haut afin de déplacer AD1 à la haute priorité.

14. Cliquez sur Submit afin de sauvegarder.

15. Confirmez que le nouvel ordre de source d'identité est ajouté.

16. Employez l'AD afin d'authentifier les mes périphériques portaiux. Naviguez vers **ISE > ordre de source de gestion >** de **Gestion de l'identité >** d'**identité**, et éditez **MyDevices_Portal_Sequence**.

17. Ajoutez **AD1 à la** liste sélectionnée, et cliquez sur le bouton haut afin de déplacer AD1 à la haute priorité.

18. Cliquez sur **Save**.

19. Confirmez que l'ordre de mémoire d'identité pour MyDevices_Portal_Sequence contient

AD1.

20. Répétez les étapes 16-19 afin d'ajouter AD1 pour Guest_Portal_Sequence, et cliquez sur la **sauvegarde**.

21. Confirmez que Guest_Portal_Sequence contient **AD1**.

22. Afin d'ajouter le WLC au périphérique d'accès au réseau (WLC), naviguez vers la **gestion >** les **ressources de réseau >** les **périphériques de réseau**, et cliquez sur Add.

23. Ajoutez le nom WLC, adresse IP, masque de sous-réseau, et ainsi de suite.

24. Faites descendre l'écran aux configurations d'authentification, et écrivez le secret partagé. Ceci doit apparier le secret partagé du RAYON WLC.

25. Cliquez sur **Submit**.

26. Naviguez vers **ISE > stratégie > éléments > résultats de stratégie**.

27. Développez les **résultats** et l'**autorisation**, cliquez sur les **profils d'autorisation**, et cliquez sur Add pour un nouveau profil.

28. Donnez à ce profil ces valeurs :

    Nom : **CWA**

    Authentification Web d'enable (la case est cochée) :

    Authentification Web : **Centralisé**ACL : **ACL-REDIRECT** (ceci doit apparier le nom d'ACL de pre-auth WLC.)Réorientez : **Par défaut**

29. Cliquez sur Submit, et confirmez que le profil d'autorisation CWA a été ajouté.

30. Cliquez sur Add afin de créer un nouveau profil d'autorisation.

31. Donnez à ce profil ces valeurs :

    Nom : **Disposition**

    Authentification Web d'enable (la case est cochée) :

    Valeur d'authentification Web : **Ravitaillement de suppliant**

    ACL : **ACL-REDIRECT** (ceci doit apparier le nom d'ACL de pre-auth WLC.)

32. Cliquez sur Submit, et confirmez que le profil d'autorisation de disposition a été ajouté.

33. Faites descendre l'écran dans les résultats, développez le **ravitaillement de client**, et cliquez sur les **ressources**.

34. **Profil indigène** choisi de **suppliant**.

35. Donnez au profil un nom de **WirelessSP** (dans cet exemple).

36. Écrivez ces valeurs :

    Type de connexion : **Radio**SSID : **Demo1x** (cette valeur est de la configuration du 802.1x WLAN WLC)Protocol permis : **TLS**Taille de clé : **1024**

37. Cliquez sur **Submit**.

38. Cliquez sur **Save**.

39. Confirmez que le nouveau profil a été ajouté.

40. Naviguez vers la **stratégie >** le **ravitaillement de client**.

41. Écrivez ces valeurs pour la règle de ravitaillement des périphériques IOS :

    Nom de règle : **IOS**Groupes d'identité : **Quels**

    Systèmes d'exploitation : **IOS tout de MAC**

    Résultats : **WirelessSP** (c'est le profil indigène de suppliant créé plus tôt)

    Naviguez vers des **résultats >** le **profil d'assistant** (liste déroulante) **> WirelessSP**.

42. Confirmez que le profil de ravitaillement IOS a été ajouté.

43. Du côté droit de la première règle, localisez la liste déroulante d'actions, et sélectionnez le **doublon ci-dessous** (ou ci-dessus).

44. Changez le nom de la nouvelle règle à **Android**.

45. Changez les systèmes d'exploitation à **Android**.

46. Laissez d'autres valeurs inchangées.

47. **Sauvegarde de** clic (en bas à gauche écran).

48. Naviguez vers **ISE > stratégie > authentification**.

49. Modifiez la condition pour inclure Wireless_MAB, et développez **Wired_MAB**.

50. Cliquez sur la liste déroulante de **nom de condition**.

51. **Dictionnaires** choisis **> état composé**.

52. **Wireless_MAB** choisi.

53. Àla droite de la règle, sélectionnez la flèche pour développer.

54. Sélectionnez ces valeurs de la liste déroulante :

    Source d'identité : **TestSequence** (c'est la valeur créée plus tôt)Si échec de l'authentification : **Anomalie**Si utilisateur non trouvé : **Continuez**Si le processus manquait : **Baisse**

55. Allez au **dot1x la** règle, et changez ces valeurs :

    Condition : **Wireless_802.1X**

    Source d'identité : **TestSequence**

56. Cliquez sur **Save**.

57. Naviguez vers **ISE > stratégie > autorisation**.

58. Des règles par défaut (telles que le par défaut noir de liste, profilé, et le par défaut) sont déjà configurées de l'installation ; les deux premiers peuvent être ignorés ; la règle par défaut sera éditée plus tard.

59. Àla droite de la deuxième règle (Téléphones IP profilés de Cisco), cliquez sur vers le bas la flèche à côté de éditent, et sélectionnent la **nouvelle règle d'insertion ci-dessous**.

    Une nouvelle règle standard # est ajoutée.

60. Changez le nom de règle de la règle standard # à **OpenCWA**. Cette règle initie la procédure d'enregistrement sur le WLAN ouvert (double SSID) pour les utilisateurs qui viennent au réseau d'invité afin de faire provisioned des périphériques.

61. Cliquez sur le plus (**+**) pour des conditions, et cliquez sur l'**état existant choisi de la bibliothèque**.

62. **Conditions composées** choisies **> Wireless_MAB**.

63. Dans le profil d'AuthZ, cliquez sur le plus (**+**), et sélectionnez la **norme**.

64. Sélectionnez le **CWA** standard (c'est le profil d'autorisation créé plus tôt).

65. Confirmez que la règle est ajoutée dans les conditions et l'autorisation correctes.

66. Clic **fait** (du côté droit de la règle).

67. Àla droite de la même règle, cliquez sur vers le bas la flèche à côté de éditent, et sélectionnent la **nouvelle règle d'insertion ci-dessous**.

68. Changez le nom de règle de la règle standard # à **PEAPrule** (dans cet exemple). Cette règle est pour le PEAP (également utilisé pour le scénario simple SSID) pour vérifier cette authentification de 802.1X sans Transport Layer Security (TLS) et ce ravitaillement de suppliant de réseau est initié avec le profil d'autorisation de disposition créé précédemment.

69. Changez la condition à **Wireless_802.1X**.

70. Cliquez sur l'icône d'équipement du côté droit de la condition, et choisi **ajoutez l'attribut/valeur**. C'est « et » condition, pas « ou » condition.

71. Localisez et sélectionnez l'**accès au réseau**.

72. **AuthenticationMethod** choisi, et écrivent ces valeurs :

    AuthenticationMethod : **Égaux**

    MSCHAPV2 choisi.

    C'est un exemple de la règle ; soyez sûr de confirmer que la condition est ET.

73. Dans le profil d'AuthZ, **norme > disposition** choisies (c'est le profil d'autorisation créé plus tôt).

74. Cliquez sur **Done**.

75. Àla droite du PEAPrule, cliquez sur vers le bas la flèche à côté de éditent, et sélectionnent la **nouvelle règle d'insertion ci-dessous**.

76. Changez le nom de règle de la règle standard # à **AllowRule** (dans cet exemple). Cette règle sera utilisée afin de permettre l'accès aux périphériques enregistrés avec des Certificats installés.

77. Dans des conditions, **conditions composées** choisies.

78. **Wireless_802.1X** choisi.

79. Ajoutez ET l'attribuez.

80. Cliquez sur l'icône d'équipement du côté droit de la condition, et choisi **ajoutez l'attribut/valeur**.

81. Localisez et sélectionnez le **rayon**.

82. **Calling-Station-ID--[31]** choisi.

83. **Égaux** choisis.

84. Allez au **CERTIFICAT**, et cliquez sur la flèche à droite.

85. **Nom alternatif soumis** choisi.

86. Pour le profil d'AuthZ, **norme** choisie.

87. **Autorisation** choisie **Access**.

88. Cliquez sur **Done**.

C'est un exemple de la règle :

89. Localisez la règle par défaut afin de changer PermitAccess à DenyAccess.

90. Cliquez sur Edit afin d'éditer la règle par défaut.

91. Allez au profil existant d'AuthZ de PermitAccess.

92. **Norme** choisie.

93. **DenyAccess** choisi.

94. Confirmez que la règle par défaut a DenyAccess si aucune correspondance n'est trouvée.

95. Cliquez sur **Done**.

    C'est un exemple des règles principales exigées pour ce test ; ils s'appliquent pour un SSID simple ou le double scénario SSID.

96. Cliquez sur **Save**.

97. Naviguez vers **ISE > gestion > système > Certificats** afin de configurer le serveur ISE avec un profil SCEP.

98. Dans des exécutions de certificat, **profils du** clic **SCEP CA**.

99. Cliquez sur **Add**.

100. Écrivez ces valeurs pour ce profil :

     Nom : **mySCEP** (dans cet exemple)URL : *<ca-server>* **/CertSrv/mscep/ de https://** (vérifiez votre configuration du serveur CA pour l'adresse exacte.)

101. Cliquez sur la **Connectivité de test** afin de tester la Connectivité de la connexion SCEP.

102. Cette réponse prouve que la Connectivité de serveur est réussie.

103. Cliquez sur **Submit**.

104. Le serveur répond que le profil CA a été créé avec succès.

105. Confirmez que le profil SCEP CA est ajouté.

Expérience utilisateur - IOS de ravitaillement

Double SSID

Cette section couvre le double SSID et décrit comment se connecter à l'invité à provisioned et comment se connecter à un 802.1x WLAN.

Terminez-vous ces étapes afin de provision l'IOS dans le double scénario SSID :

1. Sur le périphérique IOS, allez au **WiFi les réseaux**, et au **DemoCWA** choisi (WLAN ouvert configuré sur WLC).

2. Ouvrez le navigateur de safari sur le périphérique IOS, et visitez un URL accessible (par exemple, web server interne et externe). L'ISE vous réoriente au portail. Cliquez sur **Continue**.

3. Vous êtes réorienté au portail d'invité pour la procédure de connexion.

4. Procédure de connexion avec un compte utilisateur et un mot de passe d'AD. Installez le profil CA une fois incité.

5. Cliquez sur le certificat de confiance **Install du** serveur CA.

6. Cliquez sur **fait** une fois que le profil est complètement installé.

7. Revenez au navigateur, et cliquez sur le **registre**. Notez l'ID de périphérique qui contient l'adresse MAC du périphérique.

8. Le clic **installent** afin d'installer le profil vérifié.

9. Le clic **installent maintenant**.

10. Après que le processus soit terminé, le profil de WirelessSP confirme que le profil est installé. Cliquez sur **Done**.

11. Allez au **WiFi les réseaux**, et changez le réseau à **Demo1x**. Votre périphérique est maintenant connecté et utilise le TLS.

12. Sur l'ISE, naviguez vers des **exécutions >** des **authentifications**. Les événements affichent le processus dans lequel le périphérique est connecté au réseau ouvert d'invité, passe par la procédure d'enregistrement avec le ravitaillement de suppliant, et est permis l'accès d'autorisation après enregistrement.

13. Naviguez vers **ISE > gestion > Gestion de l'identité > groupes > groupes > RegisteredDevices d'identité de point final**. L'adresse MAC a été ajoutée à la base de données.

SSID simple

Cette section couvre le SSID simple et décrit comment se connecter directement à un 802.1x WLAN, fournir le nom d'utilisateur/mot de passe d'AD pour l'authentification PEAP, provision par un compte d'invité, et rebrancher avec le TLS.

Terminez-vous ces étapes afin de provision l'IOS dans le scénario simple SSID :

1. Si vous utilisez le même périphérique IOS, retirez le point final des périphériques enregistrés.

2. Sur le périphérique IOS, naviguez vers des **configurations >** des **généraux >** des **profils**. Retirez les profils installés dans cet exemple.

3. Le clic **retirent** afin de retirer les profils précédents.

4. Connectez directement au 802.1x au périphérique (effacé) existant ou à un nouveau périphérique IOS.

5. Connectez au **dot1x**, écrivez un nom d'utilisateur et mot de passe, et le clic **se joignent**.

6. Répétez les étapes 90 et en fonction de la section de configuration ISE jusqu'à ce que les profils appropriés soient complètement installés.

7. Naviguez vers **ISE > exécutions > authentifications** afin de surveiller le processus. Cet exemple affiche le client qui est connecté directement au 802.1X WLAN pendant qu'il provisioned, déconnecte, et rebranche au même WLAN avec l'utilisation du TLS.

8. Naviguez vers **WLC > moniteur > [MAC de client]**. Dans le petit groupe de client, notez que le client est dans l'état de PASSAGE, son commutateur de données est placé aux gens du pays, et l'authentification est centrale. Cela vaut pour les clients qui se connectent à FlexConnect AP.

Expérience utilisateur - Ravitaillement Android

Double SSID

Cette section couvre le double SSID et décrit comment se connecter à l'invité à provisioned et comment se connecter à un 802.1x WLAN.

La procédure de connexion pour le périphérique d'Android est très semblable à celle pour un périphérique IOS (SSID simple ou double). Cependant, une importante différence est que le périphérique d'Android exige de l'accès à Internet afin d'accéder au marché de Google (maintenant Google Play) et télécharger l'agent de suppliant.

Terminez-vous ces étapes afin de provision un périphérique d'Android (tel que le Samsung Galaxy dans cet exemple) dans le double scénario SSID :

1. Dans le périphérique d'Android, employez le WiFi afin de se connecter à **DemoCWA**, et ouvrir le WLAN invité.

2. Recevez n'importe quel certificat afin de se connecter à l'ISE.

3. Écrivez un nom d'utilisateur et mot de passe au portail d'invité afin d'ouvrir une session.

4. **Registre de** clic. Les tentatives de périphérique d'atteindre l'Internet afin d'accéder au marché de Google. Ajoutez toutes les règles supplémentaires à l'ACL de Pre-Auth (tel qu'ACL-REDIRECT) dans le contrôleur afin de permettre l'accès à Internet.

5. Google répertorie la configuration réseau de Cisco comme app d'Android. Cliquez sur **Install**.

6. Connectez-vous à Google, et le clic **INSTALLENT**.

7. Cliquez sur **OK**.

8. Sur le périphérique d'Android, trouvez l'app installé de **Cisco SPW**, et ouvrez-le.

9. Assurez-vous que vous êtes encore ouvert une session au portail d'invité de votre périphérique d'Android.

10. **Début de** clic afin de commencer l'assistant d'installation de WiFi.

11. Cisco SPW commence à installer des Certificats.

12. Une fois incité, placez un mot de passe pour la mémoire de créance.

13. Cisco SPW retourne avec un nom de certificat, qui contient la clé et le certificat utilisateur d'utilisateur. Cliquez sur OK afin de confirmer.

14. Cisco SPW continue et incite pour un autre nom de certificat, qui contient le certificat de CA. Entrez dans l'**iseca de** nom (dans cet exemple), puis cliquez sur OK afin de continuer.

15. Le périphérique d'Android est maintenant connecté.

Mes périphériques portaiux

Mon portail de périphériques permet à des utilisateurs pour mettre les périphériques sur la liste noire précédemment enregistrés qu'un périphérique est perdu ou en cas dérobé. Il permet également à des utilisateurs re-pour enrôler si nécessaire.

Terminez-vous ces étapes afin de mettre un périphérique sur la liste noire :

1. Afin d'ouvrir une session à mon portail de périphériques, ouvrez un navigateur, se connectent à https://ise-server:8443/mydevices (notez le numéro de port 8443), et à la procédure de connexion à un compte d'AD.

2. Localisez le périphérique sous l'ID de périphérique, et cliquez sur **perdu ?** afin d'initier mettre d'un périphérique sur la liste noire.

3. Quand l'ISE incite un avertissement, cliquez sur **oui** afin de poursuivre.

4. ISE confirme que le périphérique est marqué en tant que **perdu**.

5. N'importe quelle tentative de se connecter au réseau au périphérique précédemment enregistré est maintenant bloquée, même s'il y a un certificat valide installé. C'est un exemple d'un périphérique mis sur la liste noire qui échoue authentification :

6. Un administrateur peut naviguer vers **ISE > gestion > Gestion de l'identité > groupes**, **groupes d'identité de point final de** clic **> liste noire**, et voit que le périphérique est mis sur la liste noire.

Terminez-vous ces étapes afin de rétablir un périphérique mis sur la liste noire :

1. Du mon portail de périphériques, le clic **rétablissent** pour ce périphérique.

2. Quand ISE incite un avertissement, cliquez sur **oui** afin de poursuivre.

3. ISE confirme que le périphérique a été avec succès rétabli. Connectez le périphérique rétabli au réseau afin de tester qu'on permettra le périphérique maintenant.

Référence - Certificats

ISE exige non seulement un certificat racine CA valide, mais a besoin également d'un certificat valide signé par CA.

Terminez-vous ces étapes afin d'ajouter, lier, et importer le nouveau certificat de CA de confiance :

1. Naviguez vers **ISE > gestion > système > Certificats**, cliquez sur les **Certificats locaux**, et cliquez sur Add.

2. Choisi **générez la demande de signature de certificat** (CSR).

3. Écrivez le sujet **CN=<ISE-SERVER** *hostname.FQDN> de* certificat. Pour les autres champs, vous pouvez utiliser le par défaut ou les valeurs priées par votre installation CA. Cliquez sur **Submit**.

4. ISE vérifie que le CSR a été généré.

5. Afin d'accéder au CSR, cliquez sur les exécutions de **demandes de signature de certificat**.

6. Sélectionnez le CSR récemment créé, puis cliquez sur l'**exportation**.

7. ISE exporte le CSR à un fichier .pem. **Le fichier de sauvegarde de** clic, cliquent sur OK alors afin de sauvegarder le fichier à l'ordinateur local.

8. Localisez et ouvrez le fichier du certificat ISE avec un éditeur de texte.

9. Copiez le contenu entier du certificat.

10. Connectez au serveur CA, et à la procédure de connexion à un compte administrateur. Le serveur est Microsoft 2008 CA chez https://10.10.10.10/certsrv (dans cet exemple).

11. **Demande de** clic un **certificat**.

12. **Demande de certificat avancée par** clic.

13. Cliquez sur la deuxième option afin de **soumettre une demande de certificat à l'aide d'un base-64-encoded CMC ou…**.

14. Collez le contenu à partir du fichier du certificat ISE (.pem) dans le champ enregistré de demande, l'assurez que le modèle de certificat est **serveur Web**, et cliquez sur Submit.

15. Cliquez sur Download le **certificat**.

16. Sauvegardez le fichier de certnew.cer ; il sera utilisé plus tard afin de lier avec l'ISE.

17. **Des Certificats** ISE, naviguez vers les **Certificats locaux**, et cliquez sur Add **> certificat de CA de grippage**.

18. Parcourez au certificat qui a été enregistré à l'ordinateur local dans l'étape précédente,

activent les protocoles d'**EAP** et d'**interface de gestion** (des cases sont vérifiées), et cliquent sur Submit. ISE peut prendre plusieurs minutes ou plus afin de redémarrer des services.

19. Revenez à la page de renvoi du CA (https://CA/certsrv/), et cliquent sur Download un **certificat de CA, une chaîne de certificat, ou un CRL**.

20. Cliquez sur **Download CA certificate**.

21. **Sauvegardez le** fichier à l'ordinateur local.

22. Avec le serveur ISE en ligne, allez aux **Certificats**, et cliquez sur les **Certificats d'autorité de certification**.

23. Cliquez sur **Import**.

24. Recherchez le certificat de CA, activez la **confiance pour l'authentification client** (la case est cochée), et cliquez sur Submit.

25. Confirmez que le nouveau certificat de CA de confiance est ajouté.

Informations connexes

- Guide d'installation du matériel de Logiciel Cisco Identity Services Engine, version 1.0.4
- Contrôleurs de LAN sans fil de la gamme Cisco 2000
- Contrôleurs de réseau LAN fil de la gamme Cisco 4400
- Gamme Cisco Aironet 3500
- Guide de déploiement de contrôleur de branchement de radio du flexible 7500
- Bring Your Own Device - Une expérience unifiée d'authentification et d'accès constant de périphérique
- Radio BYOD avec le Cisco Identity Services Engine
- Support et documentation techniques - Cisco Systems