Option 55 de liste de demande de paramètres DHCP utilisée pour profiler l'exemple de configuration de points finaux

Contenu

Introduction

Ce document décrit l'utilisation de l'option 55 de liste de demande de paramètres DHCP comme approche alternative de profiler les périphériques qui utilisent le Cisco Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Cisco recommande que vous ayez :

- Connaissance de base du processus de découverte DHCP
- Expérience avec l'utilisation d'ISE de configurer la coutume profilant des règles

[Composants utilisés](#)

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

- Version 1.2 ISE
- IOS d'Apple

- Windows 8

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.

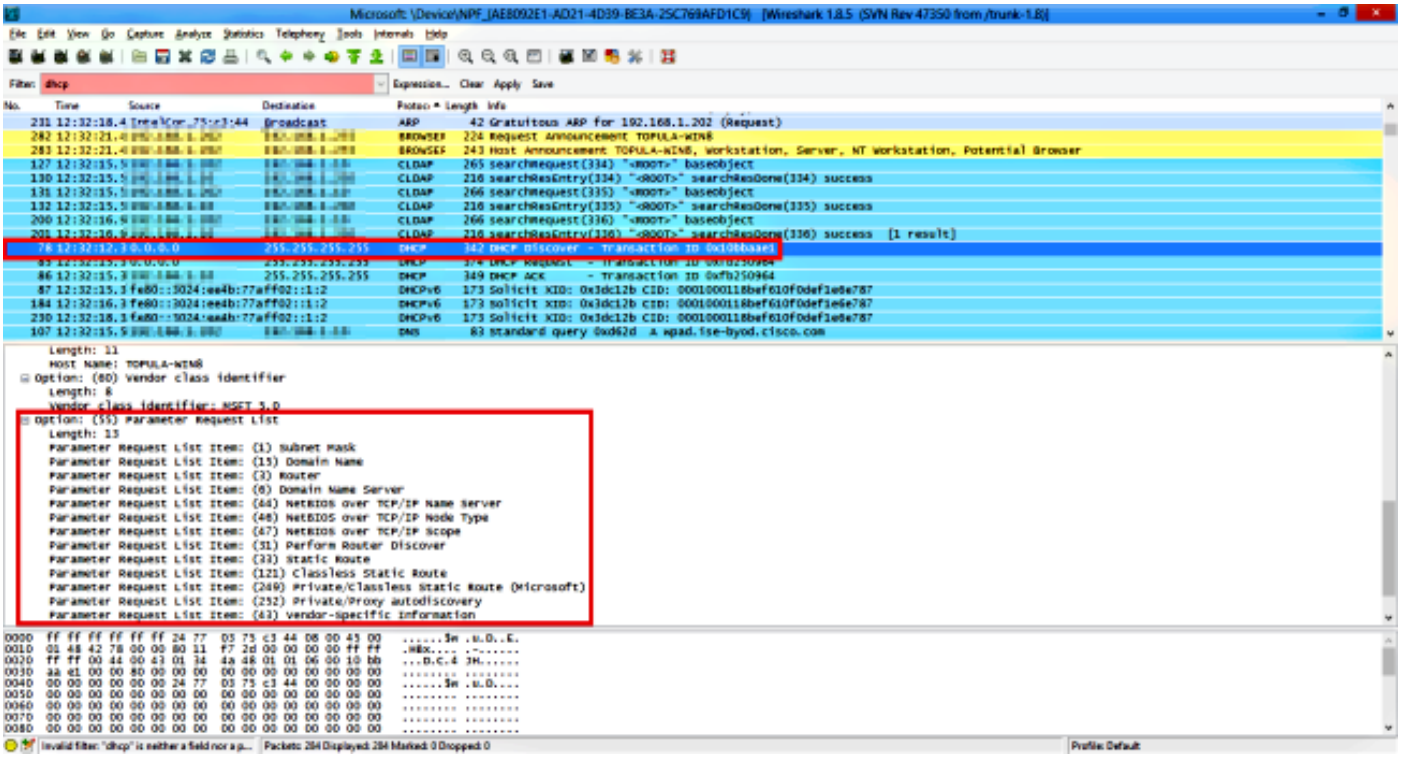
Informations générales

Dans des déploiements de la production ISE, une partie de généralement déployé profilant des sondes inclut le RAYON, le HTTP, et le DHCP. Avec la redirection URL au centre du processus ISE, la sonde de HTTP est très utilisée afin de capturer d'importantes données de point final de la chaîne d'Utilisateur-agent. Cependant, dans des quelques cas d'utilisation de production, la redirection URL n'est pas désirée et le dot1x preferered, qui le rend plus difficile de profiler exactement un point final. Par exemple, un PC des employés qui se connecte à un ensemble de services entreprise Indentifier (SSID) obtient l'accès complet tandis que son iDevice personnel (iPhone, iPad, iPod) obtient l'accès Internet seulement. Dans les deux scénarios, les utilisateurs sont profilés et dynamiquement tracés à un groupe plus spécifique d'identité pour apparier de profil d'autorisation qui ne se fonde pas sur l'utilisateur pour ouvrir un navigateur Web. Une autre alternative utilisée généralement est apparier d'adresse Internet. Cette solution est imparfaite parce que les utilisateurs pourraient changer l'adresse Internet de point final à une valeur non standard.

Dans des cas faisants le coin de ce type, la sonde DHCP et l'option 55 de liste de demande de paramètres DHCP peuvent être utilisées comme approche alternative pour profiler ces périphériques. Le champ de liste de demande de paramètres dans le paquet DHCP peut être utilisé afin de relever les empreintes digitales d'un système d'exploitation de point final tout comme un Système de prévention d'intrusion (IPS) emploie une signature afin d'apparier un paquet. Quand le système d'exploitation de point final envoie un DHCP les découvrent ou le paquet de demandes sur le fil, le fabricant inclut une liste numérique d'options DHCP qu'elle destine pour recevoir du serveur DHCP (routeur par défaut, de Domain Name Server (DN), de serveur TFTP, etc.). La commande par laquelle le DHCP Client demande ces options du serveur est assez seule et peut être utilisée afin de relever les empreintes digitales d'un système d'exploitation particulier de source. L'utilisation de l'option de liste de demande de paramètres n'est pas aussi précise que la chaîne d'Utilisateur-agent de HTTP, cependant, elle est bien plus commandée que l'utilisation des adresses Internet et d'autres données statique-définies.

> Remarque: L'option de liste de demande de paramètres DHCP n'est pas une solution parfaite parce que les données qu'elle produit sont constructeur-dépendantes et peuvent être reproduites par de plusieurs types de périphérique.

Avant que vous configuriez l'ISE profilant des règles, des captures Wireshark d'utilisation d'un point final/de Fonction Switched Port Analyzer (SPAN) ou des captures de vidage mémoire de Protocole TCP (Transmission Control Protocol) sur ISE afin d'évaluer les options de liste de demande de paramètres dans le paquet DHCP (si présent). Cette capture témoin présente les options de liste de demande de paramètres DHCP pour un PC d'entreprise de Windows 8.

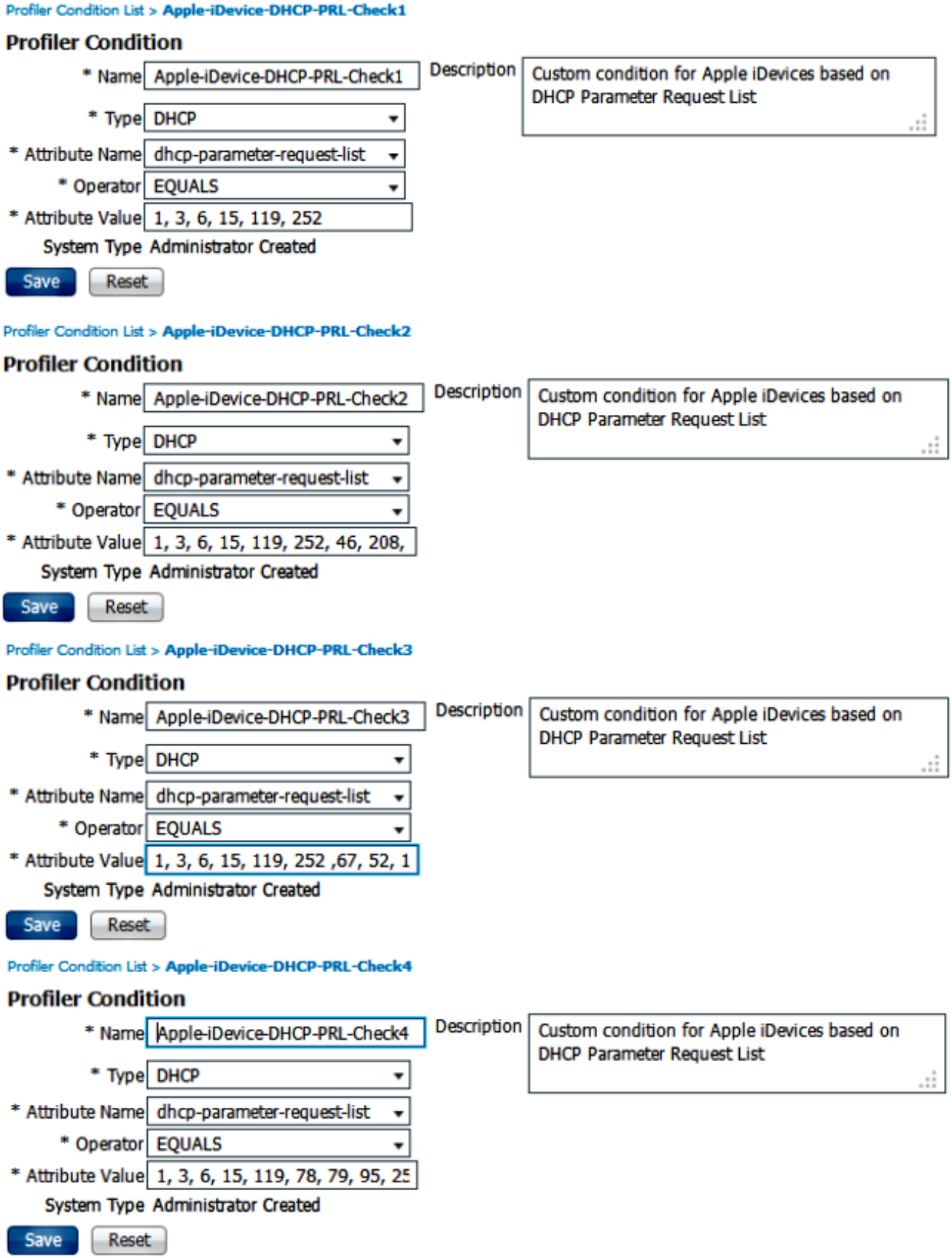


La chaîne de liste de demande de paramètres qui résulte est écrite dans le format virgule-séparé suivant : 1,15,3,6,44,46,47,31,33,121,249,252,43. Utilisez ce format en configurant la coutume profilant des conditions dans ISE.

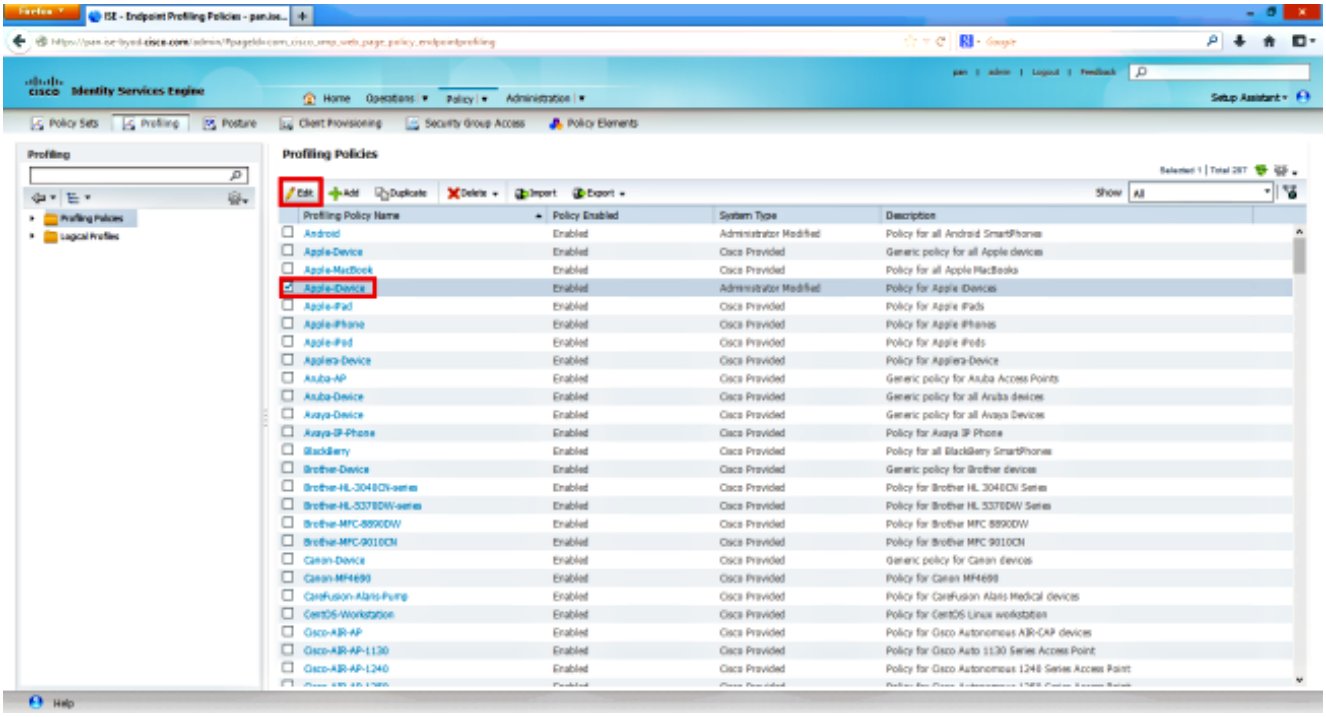
La section de configuration explique l'utilisation de la coutume profilant des conditions pour apparier des iPhones, des iPads, et des iPods dans un seul groupe d'identité appelé **Apple-iDevice**. À la différence de la chaîne de liste de demande de paramètres qui est seule à Windows 8, Apple utilise un ensemble commun de chaînes à travers de plusieurs types de point final. Pour cette raison, il n'est pas possible de différencier le type d'iDevice d'Apple avec l'utilisation seule de l'option de liste de demande de paramètres. C'est une configuration acceptable dans des déploiements de la production ISE parce que la même stratégie d'autorisation est typiquement appliquée aux iPhones, aux iPads, et aux iPods.

Configurez

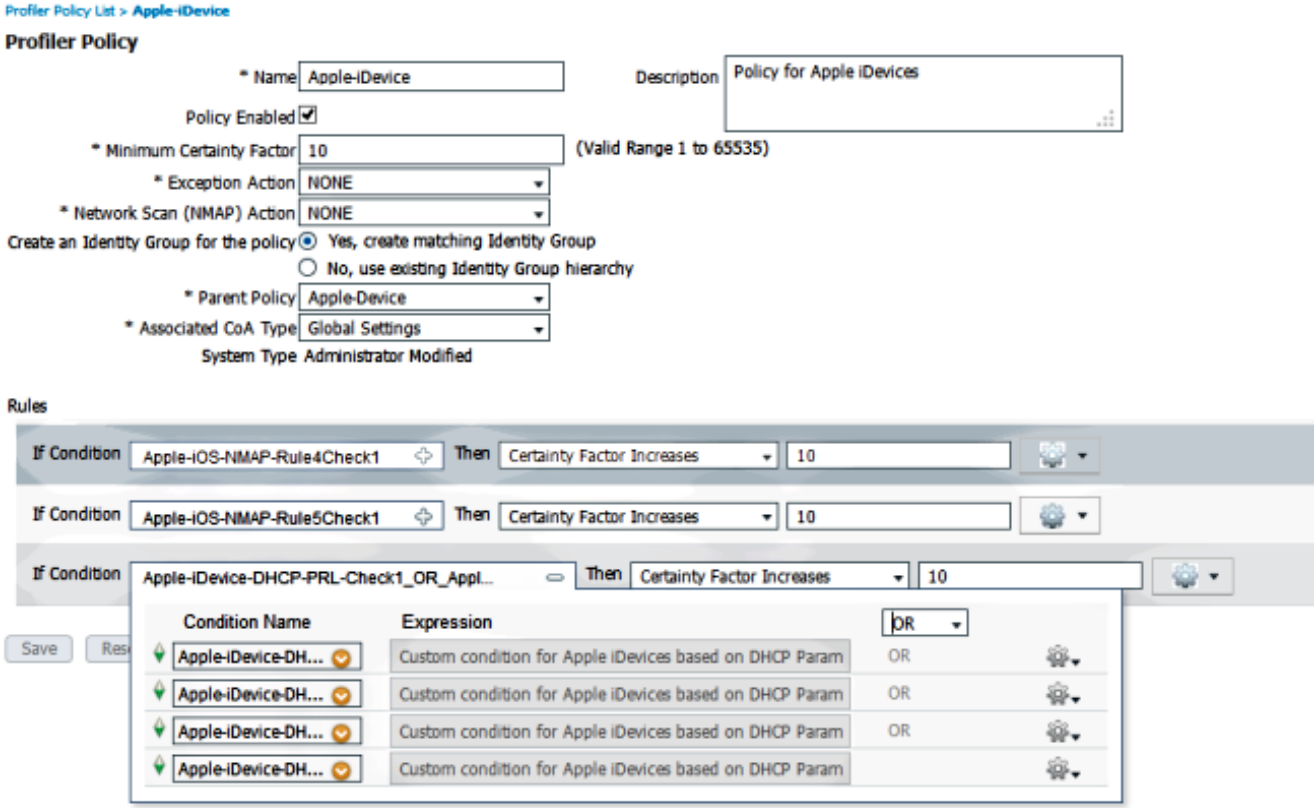
1. Ouvrez une session au GUI d'admin ISE et naviguez vers la **stratégie > les éléments > les états de stratégie > en profilant**. Cliquez sur Add afin d'ajouter un nouvel état de profilage fait sur commande. Dans cet exemple, quatre seules règles sont définies pour les empreintes digital de liste de demande de paramètres d'iDevice d'Apple les plus utilisées généralement. Référez-vous à Fingerbank.org pour une liste complète de valeurs de liste de demande de paramètres.
   Remarque: La zone de texte de **valeur d'attribut** ne pourrait pas présenter toutes les options numériques, et vous pourriez devoir faire défiler avec la souris ou le clavier afin de visualiser la liste complète.



2. Les conditions de coutume étant défini, naviguez vers la **stratégie > en profilant > en profilant Polcies** afin de modifier un courant profilant la stratégie ou afin de configurer un neuf. Dans cet exemple, la stratégie d'**Apple-iDevice de** par défaut est éditée afin d'inclure les nouveaux conditions de liste de demande de paramètres.



3. Ajoutez un nouvel état composé à la règle de stratégie de profileur d'**Apple-iDevice** et assurez-vous qu'**OU l'**opérande est sélectionné de sorte que les chaînes configurées l'unes des de liste de demande de paramètres puissent avoir comme conséquence une correspondance. Modifiez le **facteur de certitude** au besoin afin de réaliser le résultat de profilage désiré.

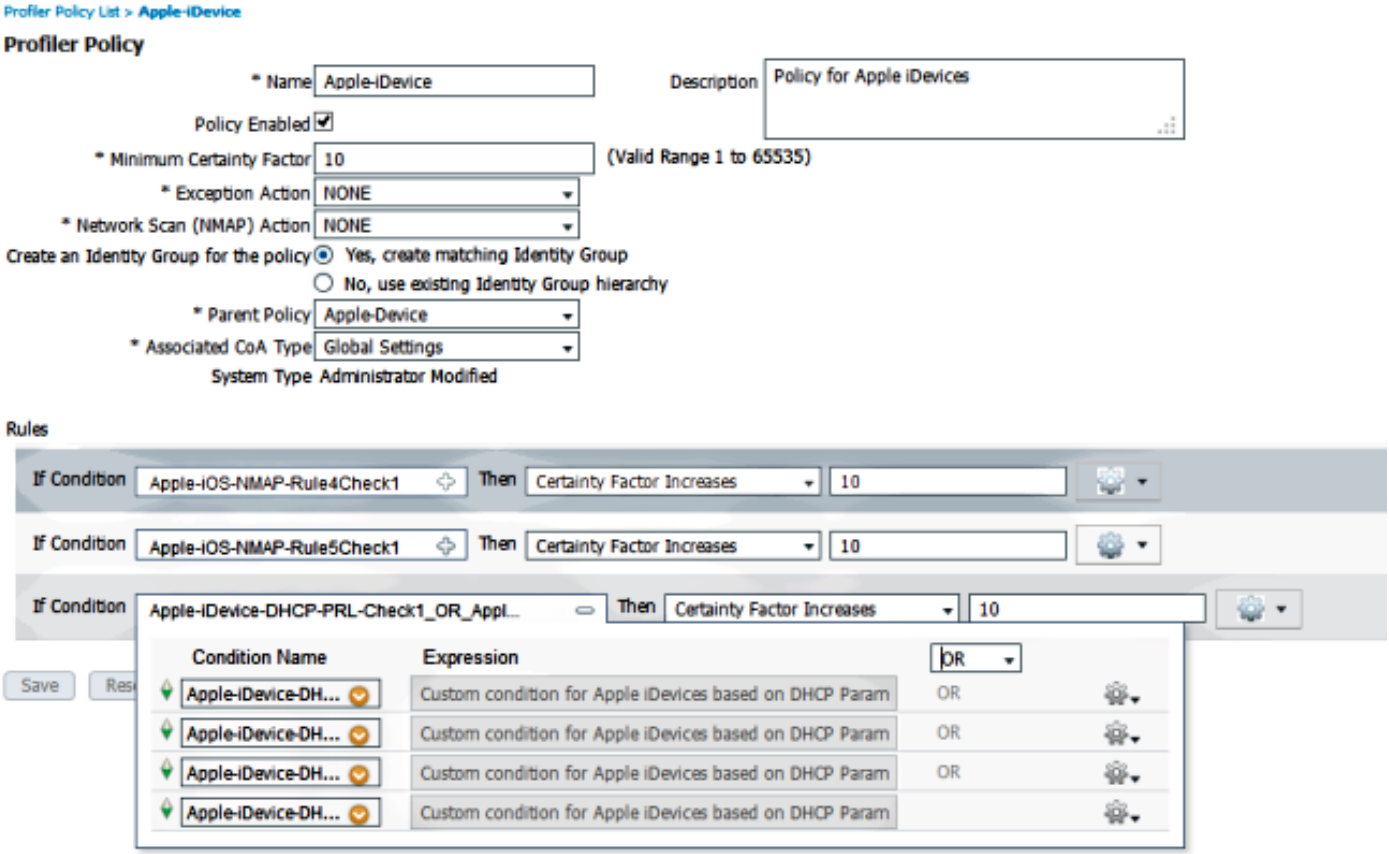


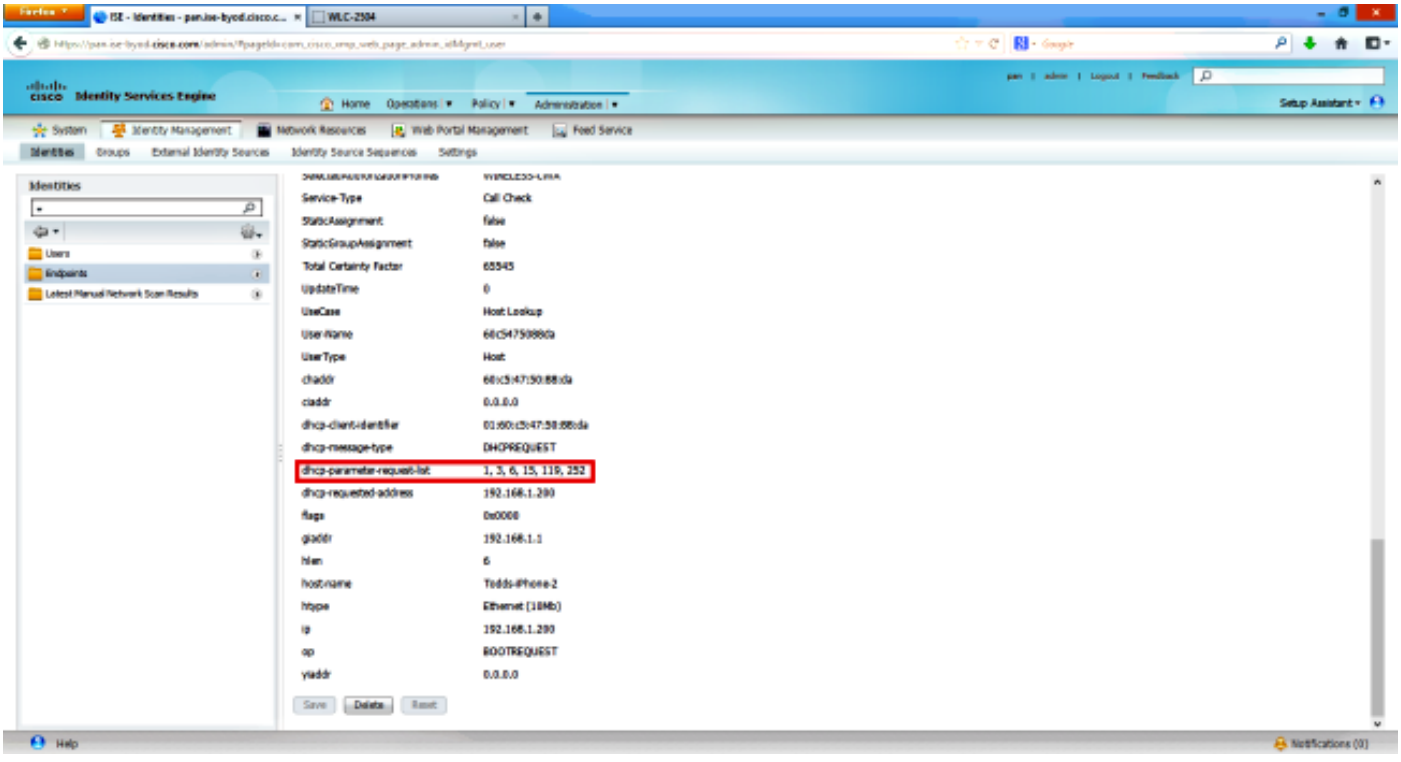
Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- Naviguez vers la **gestion > la Gestion de l'identité > les identités > les points finaux** et éditez le **profil de point final** pour le périphérique/adresse MAC.
- Confirmez que l'**EndPointPolicy** est Apple-iDevice, que l'**EndPointSource** est sonde DHCP, et que la DHCP-paramètre-demande-**liste** évalue la correspondance les valeurs de condition précédemment a configuré.





L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes**

show. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Vérifiez que les paquets DHCP ont atteint les Noeuds de stratégie ISE qui remplissent la fonction de profilage (avec le helper-address ou l'ENVERGURE).
- Utilisez les **exécutions > dépannent > des outils de diagnostic > les outils généraux >** outil du **vidage mémoire de TCP** ? afin d'exécuter à la façon des indigènes des captures de vidage mémoire de TCP du GUI d'admin ISE.
- Référez-vous à la base de données d'empreinte digital DHCP de Fingerbank.org pour une liste en cours d'options de liste de demande de paramètres.
- Assurez-vous que les valeurs correctes de liste de demande de paramètres sont configurées dans l'ISE profilant des conditions. Certaines des chaînes généralement utilisées incluent :

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

> Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

Informations connexes

- Base de données d'empreinte digital DHCP de Fingerbank.org
- Support et documentation techniques - Cisco Systems