Understand Umbrella Roaming Client Dashboard Reports

Contents

Introduction

This document describes how to understand under which scenarios you can see information from the identity for a Cisco Umbrella Roaming Client.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella Roaming Client.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

There are several cases in which searching for a Cisco Umbrella roaming client in the **Filter by Identity** field of the **Reporting** section of the Umbrella dashboard can yield different results than you expect. This article can help you understand under which scenarios you can see information from the identity for an Umbrella roaming client.

The Umbrella roaming client is also referred to as Roaming Computers in the dashboard reporting.

Normally, you can see an Umbrella roaming client's status for reporting be shown under the identity for that Umbrella roaming client. However, depending on where the Umbrella roaming client is in regard to the network and the way policy is set, the exceptions are described in this article.

Virtual Appliances and Active Directory

If the Umbrella roaming client is connected to a network with Virtual Appliances (VAs), the Umbrella roaming client automatically disables itself, and you do not have the ability to search Reports for that Umbrella roaming client identity. You can search by the Active Directory user, computer, or the Internal IP address of the computer.

You can tell if you are being protected by a VA by looking in the tray icon (Mac or Windows), or by checking the security status in the Umbrella dashboard at **Identities > Roaming Computers.**

Screen_Shot_2017-08-14_at_2.58.18_PM.png

Disable Behind Protected Networks

If the Umbrella roaming client is being protected by a network (that has been added to your Umbrella dashboard) via the Disable Behind Protected Networks feature, the Umbrella roaming client essentially disables itself and does not show up as coming from the Umbrella roaming client in the dashboard. There is no way to filter granularly.

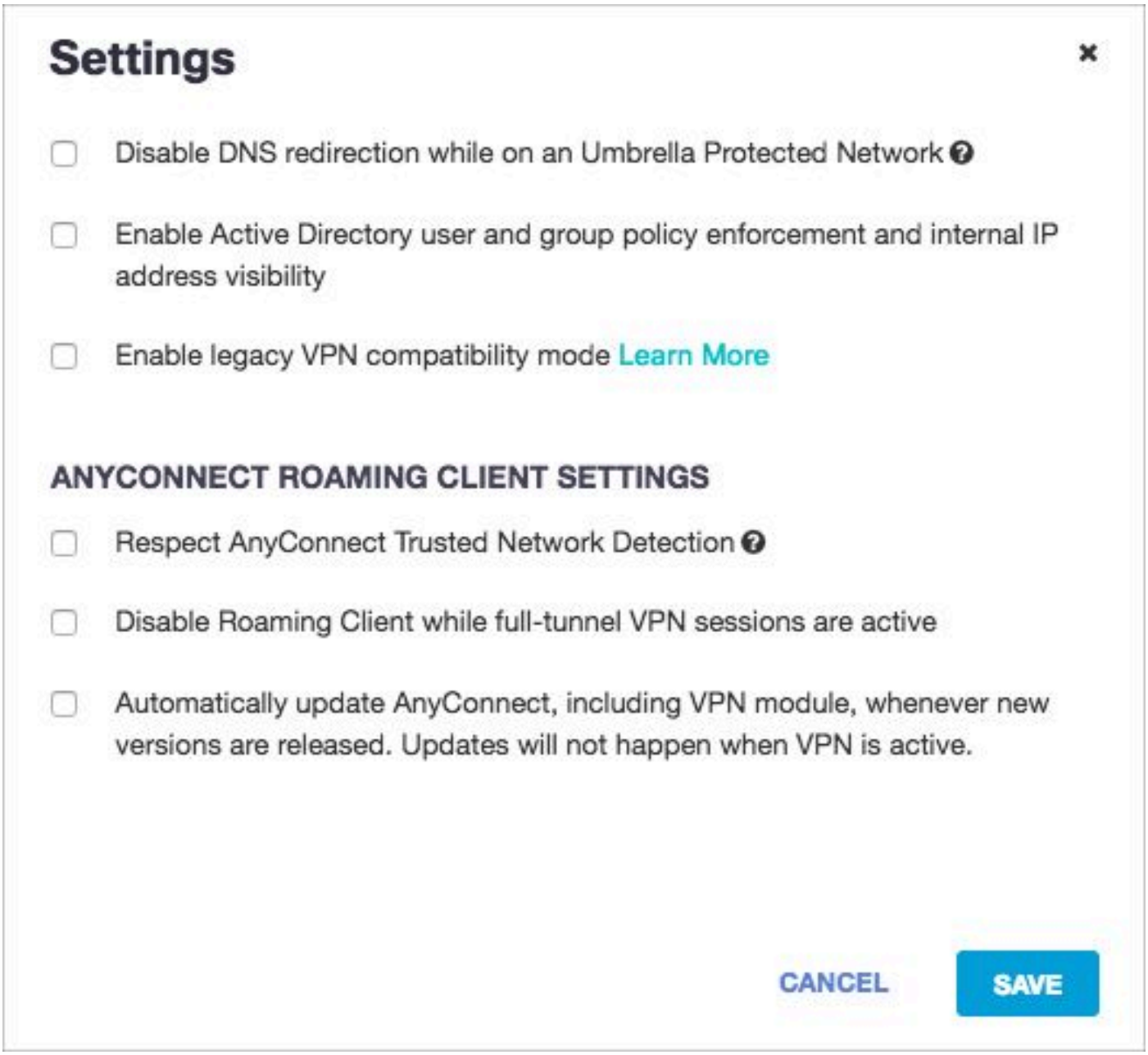
To enable or disable this feature:

1. Navigate to **Identities** > **Roaming Computers**.

2. Select the**Roaming client settings** icon.

3. Select the **Disable DNS redirection while on an Umbrella Protected Network** setting.

4. Select **Save**.



roaming_computer_settings.jpg

Policy Hierarchy

If the Umbrella roaming client is set **not** to disable via the Disable Behind Protected Networks feature but is behind an Umbrella network wherein the network's policy is higher in the Policy Hierarchy than the Umbrella roaming client, you can search for the Umbrella roaming client. However, the **Identity** in the **Reporting** section displays as the network in question, but in reality it is showing you the Umbrella roaming client's reports. In this case, the identity which shows up in Reports reflects which policy was used to enforce the content filtering or security settings.

In this example, you can search for an Identity, but instead of showing the identity in the **Identity** field in reporting, it is showing the Network of the policy for which it matched.

policy_hierarchy.jpg