Use Umbrella Active Directory Connector for Authentication

Contents

Introduction

This document describes how to use the Umbrella Active Directory Connector for authentication via 802.1x, Radius, or ISE.

Overview

The Cisco Umbrella Active Directory (AD) Connector works by mapping AD users/computers to internal IP addresses. For the mapping to be correct, AD users must authenticate against a Domain Controller that's been configured to communicate with a Cisco Umbrella AD Connector.

If your AD users authenticate through other means, a login event might not be generated on the Domain Controller at all, or there might be an unexpected mapping that results in the wrong policy being applied.

Authentication via 802.1x, RADIUS, or ISE

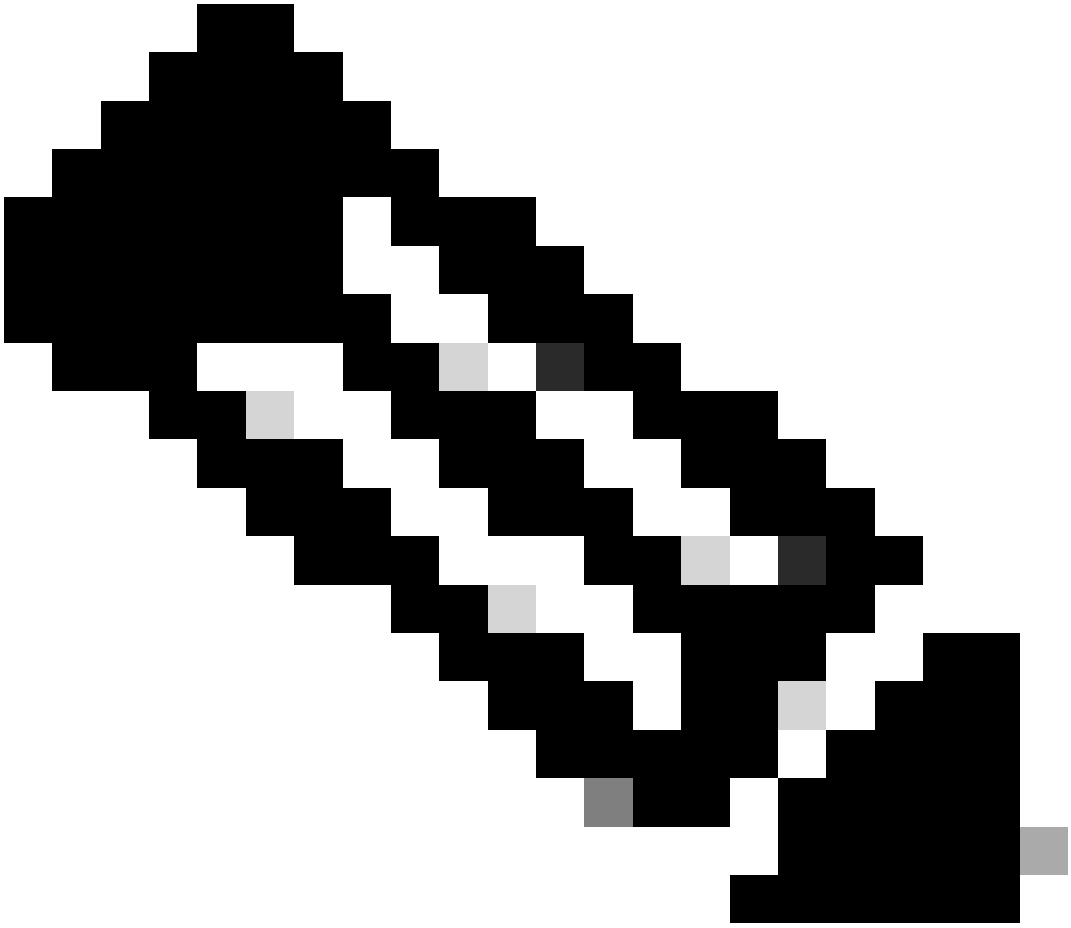
Authentication through 802.1x, RADIUS, or ISE is **not** supported due to the limitations of how Active Directory logins work with these solutions. The logon events that the AD Connector looks for are often not generated.

Read more about the Event IDs that the AD Connector looks for here: Which Window Events/EventIDs is the Connector service looking for?

Most commonly, the IP address of the authentication service is mapped to the AD user instead of the IP address of the user's computer.

Alternative Solutions

AD integration can also be achieved by the use of the roaming client with the identity support feature enabled. Further information on this feature can be found in our deployment documentation.



Note: This solution requires that virtual appliances are not present on the network, as this causes the roaming client to move into a disabled "behind VA" state.

If virtual appliances are used in the network, internal IP addresses can be used for identification. For example, you could create an "internal network" identity for the address range of your wireless network and then apply a policy to this identity. The only downside to this method is that all devices in this address range receives the same policy.