Apply Policies for Local Accounts in Umbrella Active Directory

Contents

Introduction

This document describes expected policy behavior when synchronizing Umbrella on-premise products with Active Directory and local user accounts.

Umbrella Virtual Appliance and Local Account Identification

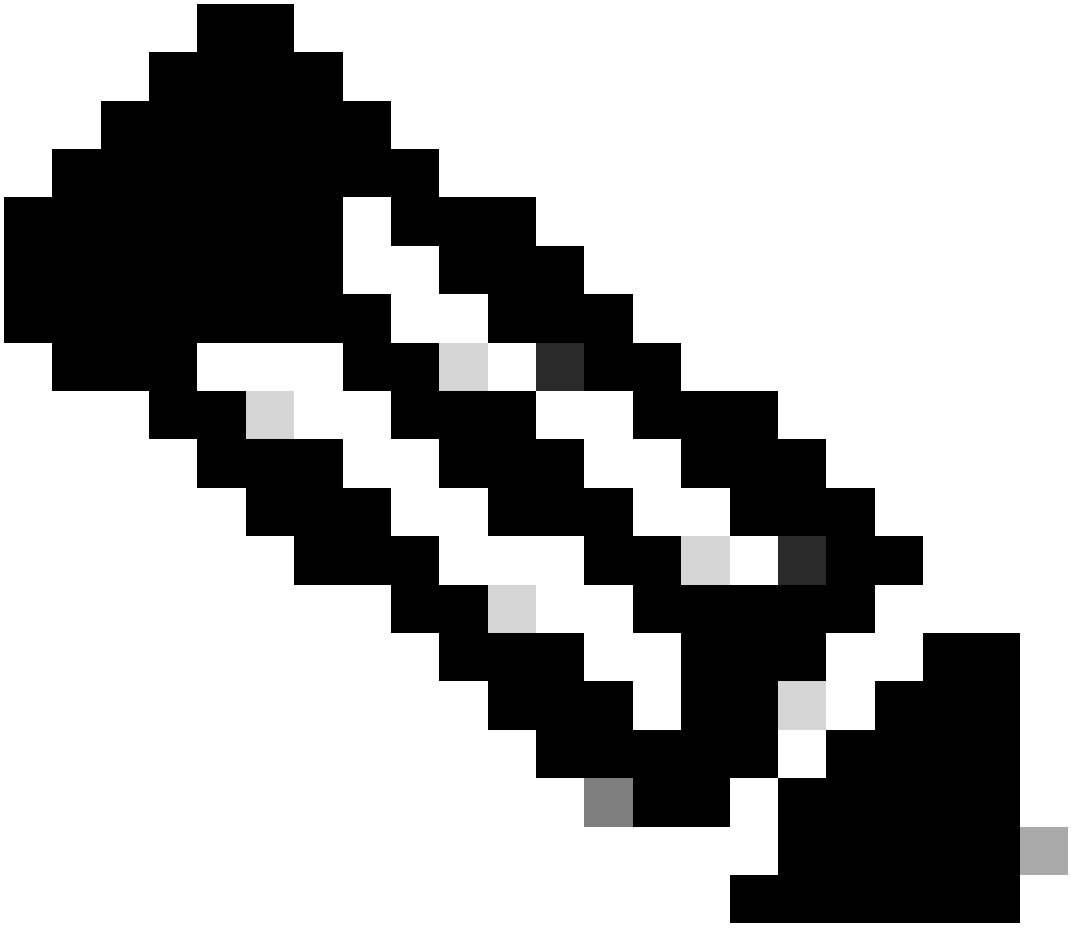
The Umbrella Virtual Appliance receives Active Directory logon information from Windows Domain Controllers. It caches and identifies Active Directory users based on their source IP address.

- The Domain Controller does not track local user logons, so these users cannot be directly identified by the Virtual Appliance.
- If an Active Directory user recently logged in from an IP address, the cached identity can still be used based on our cache. The Virtual Appliance has no way of knowing the AD user has been replaced with a local account.
- If no cached user is present, the Virtual Appliance uses a default (non-AD) identity. The identity triggered can be either:
  - Umbrella Site name (for example, Default Site)
  - Internal Network (internal IP address)
  - Network (external IP address)

Recommendations for Umbrella Virtual Appliance

- Restrict access to local accounts and passwords.
- Create a separate policy for the Umbrella site name (for example, Default Site). Assign this policy a lower priority than your standard Active Directory user policy. This more restrictive policy applies when no AD user is detected.
- If you require different policies for local user accounts, consider deploying the Umbrella Roaming Client.

Umbrella Roaming Client and Local Account Policy



Note: To use Active Directory integration with the Roaming Client, navigate to **Identities** > **Roaming Computers** and enable the setting **Enable Active Directory user and group policy enforcement**.

The Roaming Client detects logged-on users from the Windows registry, enabling identification of Active Directory users by their unique AD GUID.

- The Roaming Client cannot identify local usernames for policy purposes.
- When an AD user is detected, the AD user identity applies to policy enforcement, including AD users logged in with cached credentials while off-network.
- If no AD user is detected (for example, when a local user is logged on), the Roaming Computer identity is used for policy enforcement.

Recommendations for Umbrella Roaming Client

- Restrict access to local accounts and passwords.
- Create a separate policy for**Roaming Computers**with a lower priority than your standard AD User policy. This policy applies to Roaming Computers not joined to the Domain or used by local users.