Understand how to Lock Down the Umbrella Roaming Client in AD

Contents

Introduction

This document describes how to lock down the Umbrella Roaming Client on an Active Directory (AD) environment using Group Policy Objects (GPOs).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Umbrella Roaming Client

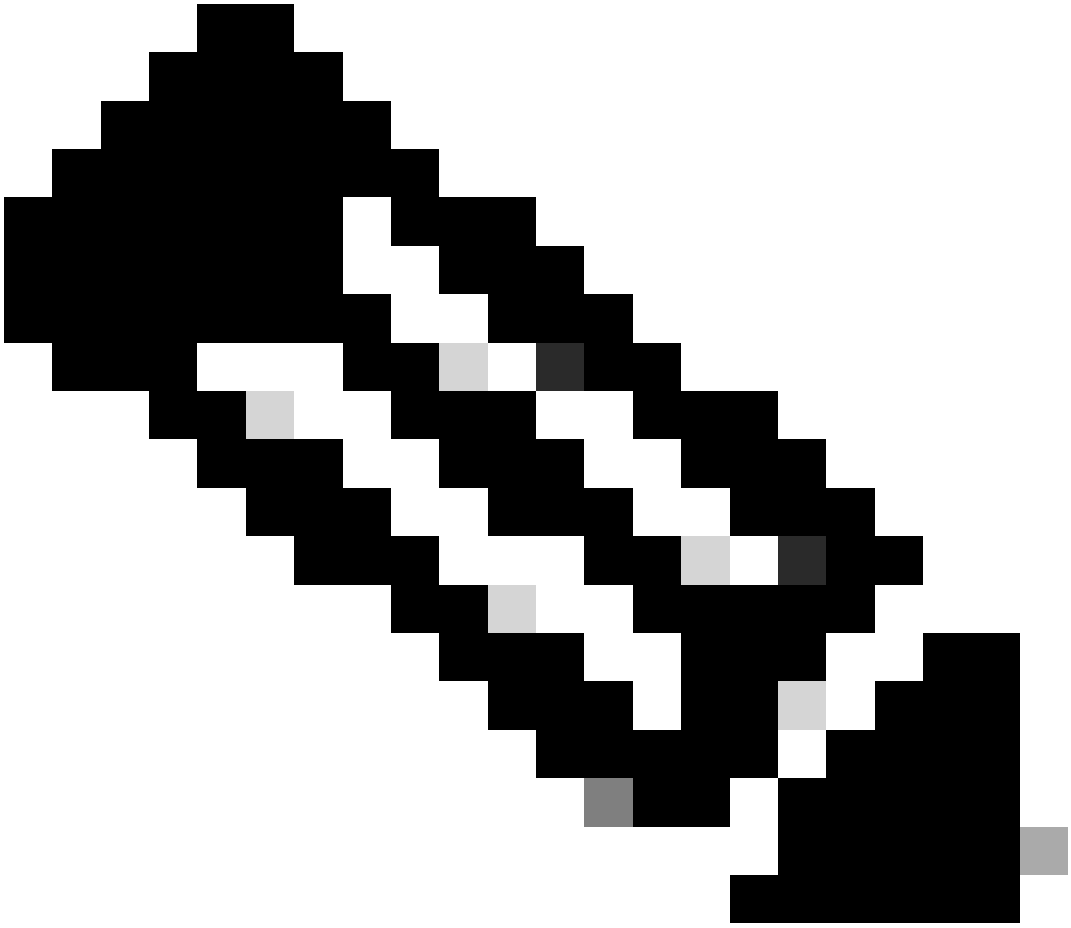
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

You want to make sure users with local administrative permissions cannot disable the Umbrella Roaming service.

Process

Complete these steps on a Windows 2003/2008 Domain Controller:



Note: If the service that you want to configure is not present in the list, you must install GPMC on a computer that has the service running.

---

1. Create a New Security Group in Active Directory called **Umbrella_Roaming**.

- This is required as you can already have a security group that contains different members of Domain Admins.

2. Open the **Group Policy Editor** (**Start > Run > Type:** `gpmc.msc` >) and create a New Group Policy object called **Umbrella**.

3. Edit the new group policy and navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > System Services**.

- The `Umbrella Roaming Client service` needs to be imported before you can see it under `System Services`. Read more about how to complete this process in this Microsoft article.

4. Scroll through the listed services until you reach the **Umbrella Roaming Client** service.

- Once policies configuration is completed, ensure the client is updated with `gpupdate` command before

testing.

5. Configure the service by double-clicking on the service name, select **Define this policy > Automatic**, and then edit the security groups.

6. Add the account **Network Service** and grant **Read** permissions. Remove the Administrators and/or Domain Administrators group as required.

Warning: DO NOT remove the SYSTEM or INTERACTIVE accounts from the list.

You can now apply the group policy to required containers in the normal way and allow the policy to be applied to the client computers.

You can test the functionality by enabling the GPO and logging onto a client computer as an administrator or as an account with group permissions that you have restricted. Attempting to stop the service can result in this message being displayed:

```
Could not stop the service on Local Computer. Error 5: Access is denied.
```

Alternatively, the option to stop the service is grayed out and unavailable. Either of these shows that the GPO has been configured and applied to the client successfully.

If the error message is not shown and you are still able to stop a restricted service, check that the GPO has been configured correctly and that there are no conflicting GPOs. For more information, consult Microsoft documentation.

Ensure that the relevant admins are added to the Umbrella_Roaming group and the service GPO allows access to the Umbrella_Roaming group.