Enable Cisco Umbrella with iCloud Private Relay

Contents

Introduction

About iCloud Private Relay

iCloud Private Relay and Cisco Umbrella

iCloud Private Relay and Cisco Umbrella with the Cisco Security Connector App

Introduction

This document describes a configuration to enable Umbrella functionality on iCloud Private Relay.

About iCloud Private Relay

iCloud Private Relay is a service provided by Apple as part of a subscription iCloud product. This enables an Apple device to protect its DNS and web traffic against tracking. This service is optional for Apple devices and requires a subscription to be active.

iCloud Private Relay and Cisco Umbrella

iCloud Private Relay overrides Umbrella functionality when activated. In order to maintain coverage on enterprise networks, a canary domain can be configured on network as per the instructions on this Apple support page.

MDM on macOS and Supervised iOS

To disable iCloud Private relay, push this payload with a value of false.

```
allowCloudPrivateRelay
```

All other devices

To prevent iCloud Private Relay from activating on a network, set the domains to respond with a NXDOMAIN or NODATA response:

```
mask.icloud.commask-h2.icloud.com
```

Once set, iCloud Private Relay users are informed that "Private Relay is turned off for 'network name'", and are not permitted to utilize iCloud Private Relay on this network.

Enforcing with Umbrella in Limited Availability

Umbrella is capable of setting this override for your organization. To request this, send us a message at umbrella-support@cisco.com. When overriding the iCloud domains with a NODATA response, any match for content categorization supersedes and returns a block page IP. This affects the user experience and can cause timeouts on macOS and iOS devices. After the override is configured, add these domains to an Allow List for all relevant policies:

```
mask.icloud.commask-h2.icloud.com
mask-api.icloud.com
mask.apple-dns.net
```

iCloud Private Relay and Cisco Umbrella with the Cisco Security Connector App

Unlike devices without Umbrella installed who receive network level coverage, all DNS requests continue to be logged to Umbrella; however, the canary domain is required to ensure that DNS blocks are not proxied by iCloud Private Relay and overridden.