Best Practices for Cisco Umbrella Users

Contents

Introduction

Cisco Umbrella Service Health and System Status

Network Registration

Local Firewalls and Proxies

The Rollout Phase

Intelligent Proxy / Block Page

Cisco Umbrella Virtual Appliances

Third Party Integrations

Active Directory Integration

Roaming Clients

Logging

Managed Services Console Best Practices

Two Factor Authentication

Contact and Work with the Cisco Umbrella Support Team

Introduction

This document describes various best practices related to Cisco Umbrella.

Cisco Umbrella Service Health and System Status

- Bookmark http://208.69.38.170/ and https://146.112.59.2/#/ so you can check the Umbrella System Status pages even if local DNS is not available.
- Subscribe to the Cisco Umbrella Service Status page at https://146.112.59.2/#/ to receive notifications about Service Degradations, Service Outages, and/or Maintenance & Events.
- Follow the Service Updates and Announcements pages of the Cisco Umbrella Knowledge Base.
- Periodically check the Cisco Umbrella Dashboard "Message Center" for product alerts and notifications.

Network Registration

All IP addresses and IP address CIDR ranges associated with your organization must be registered with Umbrella. For more information, please see the Umbrella documentation.

Local Firewalls and Proxies

- Configure local firewalls to allow Umbrella IP address CIDR ranges.
- If using an HTTP proxy, make sure it is configured.

The Rollout Phase

- Where possible, roll out gradually and test before deploying en masse. To test new functionality, apply a policy to a subset of users and computers. If the test is successful, apply the policy to more users and computers.
- Use the Policy Tester to verify intended policy functionality for identities and individual domains.
- Verify functionality by visiting test pages with a browser. For details, see: How To: Successfully test to ensure you are running Umbrella correctly.
- Create one or more Scheduled Reports to help monitor your environment for security-related events. For details about this, see the Umbrella documentation.

Intelligent Proxy / Block Page

- Include the Root CA in your rollout, especially if using or planning to use the Intelligent Proxy features. It is also a good idea to install it anyway, as sites blocked when they are https:// (eg: https://facebook.com) generate errors without it.

Cisco Umbrella Virtual Appliances

- If using virtual appliances (VA's), make sure the Internal Domains list is filled out in advance of deploying.
- If using virtual appliances on VMWare, use VMXNET3 adapters as per.
- If using virtual appliances, periodically check each VA's console via the VMWare or Hyper-V host. On the right side, all Services and Connectivity entries display as green.
- Configure internal DNS servers as detailed here: What is the recommended configuration for internal DNS Servers when Deploying Umbrella?

Third Party Integrations

- If using integrations such as Check Point or Cisco AMP Threat Grid, add any domains you wish to never have blocked to the Global Allow List (or to other domain lists as per your Umbrella policies):
  - The home page for your organization (mydomain.com).
  - Domains representing services you provide that could have both internal and external records (mail.myservicedomain.com, portal.myotherservicedomain.com).
  - There could be lesser-known cloud applications you depend on heavily that Cisco Umbrella is aware of or does not include in their automatic domain validation (localcloudservice.com)

Active Directory Integration

- If Cisco Umbrella is integrated with Active Directory, add service accounts to the AD User Exceptions list.

Roaming Clients

- If using Roaming Clients, make sure the Internal Domains list is filled out.
- Make sure that all your Roaming Clients are on the same version on the Cisco Umbrella Dashboard at **Identities > Roaming Computers**.
- If using Cisco Secure Client (formerly AnyConnect), use the Umbrella Roaming Security Module rather than the standalone Roaming Client.
- If using a Roaming Client on an Airline wifi, see Roaming Client and Airline/Hotel WiFi Best Practices.

Logging

Detailed logs are only kept for 30 days, then they are broken down into aggregated report data. If you wish to keep a copy of the more detailed data longer than 30 days, set up an Amazon S3 bucket to export your data to at **Settings > Log Management**.

Managed Services Console Best Practices

Managed Services Console MSP Professional Services Automation (PSA) Integration:

- If you are an MSP integrated with a PSA, verify that the "PSA INTEGRATION" icon displays as green.

Two Factor Authentication

- Implement two factor authentication for Cisco Umbrella users.
- Implement two-step authentication for Cisco Umbrella MSP administrators.

Contact and Work with the Cisco Umbrella Support Team

- After logging in to the Umbrella dashboard, submit a request to the Umbrella support team via the webform on the request page.
- If you have purchased telephone support from Cisco Umbrella, you see a telephone icon at the top right corner of the Cisco Umbrella Dashboard. Click on the telephone icon to display the telephone number for Support.
- Provide complete details about your problems or questions.
- Use the output of the Umbrella Diagnostic Tool for your Support case.