Integrate Secure Access with On-Premises DLP Using Secure ICAP

Contents

Introduction

This document describes how to integrate Secure Access with on-premises Data Loss Prevention (DLP) servers using Secure ICAP.

Overview

You can integrate Umbrella with your on-premises DLP solution for centralized event management and remediation workflows. This integration uses Secure ICAP (Internet Content Adaptation Protocol) to forward HTTP/S traffic that violates DLP policies to your on-premises DLP server for further analysis.

Integrate Secure Access with On-Premises DLP Servers

- Integration uses Secure ICAP, which securely transfers HTTP/S traffic that violates DLP policies to your on-premises DLP server for additional inspection.
- Secure ICAP encrypts traffic using TLS and authenticates your DLP server with a certificate uploaded in the Umbrella dashboard.
- Restrict inbound firewall rules to allow only traffic from Umbrella IP addresses to your DLP server’s ICAP port for enhanced security.

Required IP Addresses to Allow

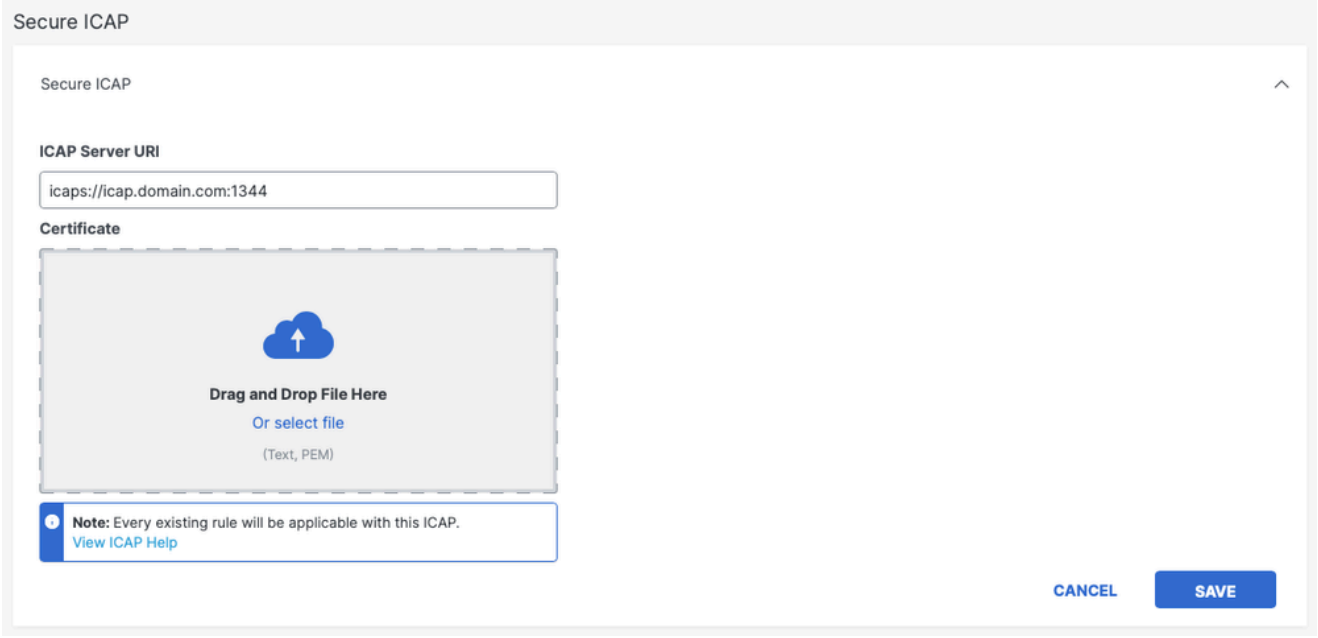
Add these Umbrella IP addresses to your firewall to allow Secure ICAP traffic:

- 50.18.191.74
- 54.153.85.86
- 54.90.48.200
- 3.234.7.118

Enable Secure ICAP Integration

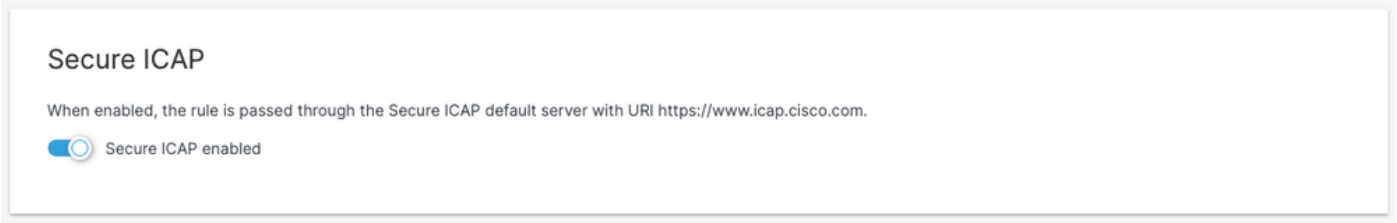
1. Onboard your on-premises DLP server:

    - In the Umbrella dashboard, go to**Admin > Authentication > ICAP**.
    - Upload the DLP server certificate to enable Secure ICAP.



2. Configure Realtime DLP rules to forward traffic to the on-premises DLP server:

    - In the rule configuration, use the**ICAP**section to enable forwarding.
    - All Realtime DLP active rules are enabled by default.



Data Sent to On-Premises DLP Server

- Umbrella sends the entire HTTP/S message (body and headers) to the on-premises DLP server.
- Custom headers are included:
    - **X-Authenticated-User:**User identity
    - **X-Authenticated-Groups:**User group identity
    - **X-Client-IP:**Client IP address

Supported Violation Events

Both monitored and blocked Realtime DLP violation events are sent over Secure ICAP.

Enable ICAP on Your DLP Server

Consult your DLP solution documentation and support to enable the embedded ICAP server. If only ICAP (not Secure ICAP) is supported, deploy a TLS termination component (such as Stunnel) in front of your On-Premises DLP server to enable Secure ICAP.

Related Resources

Refer to Umbrella documentation for additional guidance: Manage Secure ICAP