# Configure DLP and CASB Support for Generative AI and ChatGPT

## Contents

[Introduction](#)

[Overview](#)

## Introduction

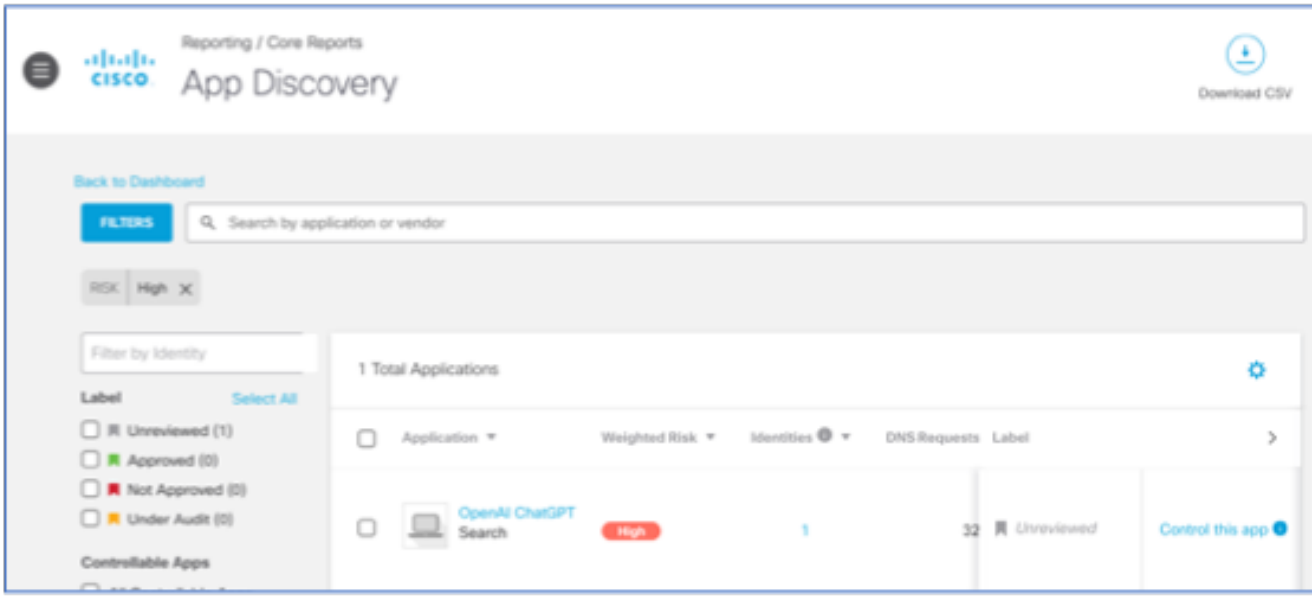
This document describes Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP) support for Generative AI and ChatGPT.

## Overview

We have released new Cloud Access Security Broker (CASB) and Data Loss Prevention (DLP) enhancements to our Umbrella product suite, designed to help customers manage ChatGPT usage within their organizations more effectively.
These enhancements enable our customers to ensure that their employees are using ChatGPT responsibly and securely while protecting sensitive information from potential risks.

Here are the key features:

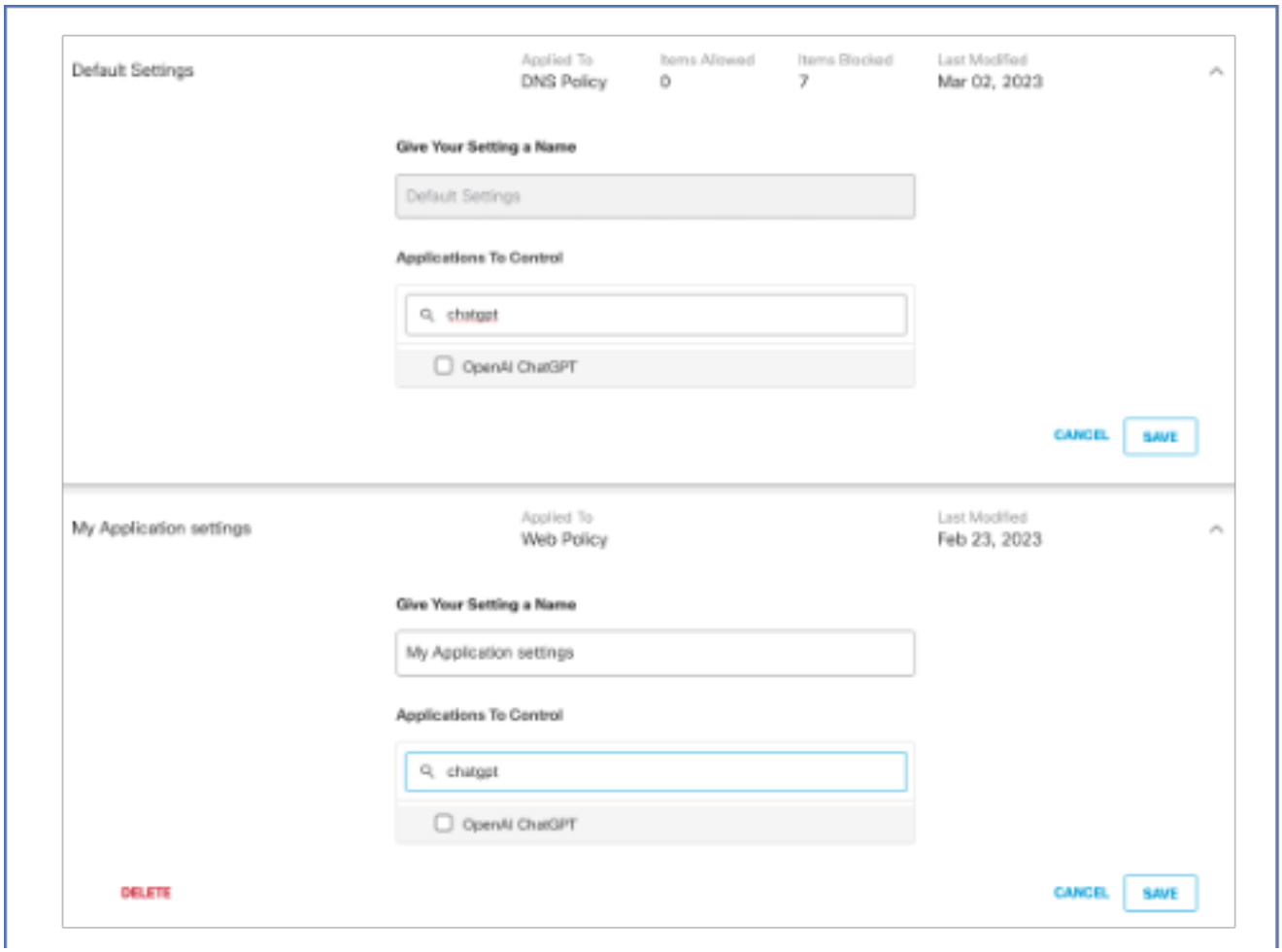
1. **Discovering ChatGPT usage in the organization:**
   Using the App Discovery report (Reports -> Core Reports), customers can identify and monitor ChatGPT usage across their organization.
   This provides them with valuable insights into how the employees are using the tool, enabling them to optimize its usage and ensure compliance with their internal policies.




*16221272854164*


*16221291406100*

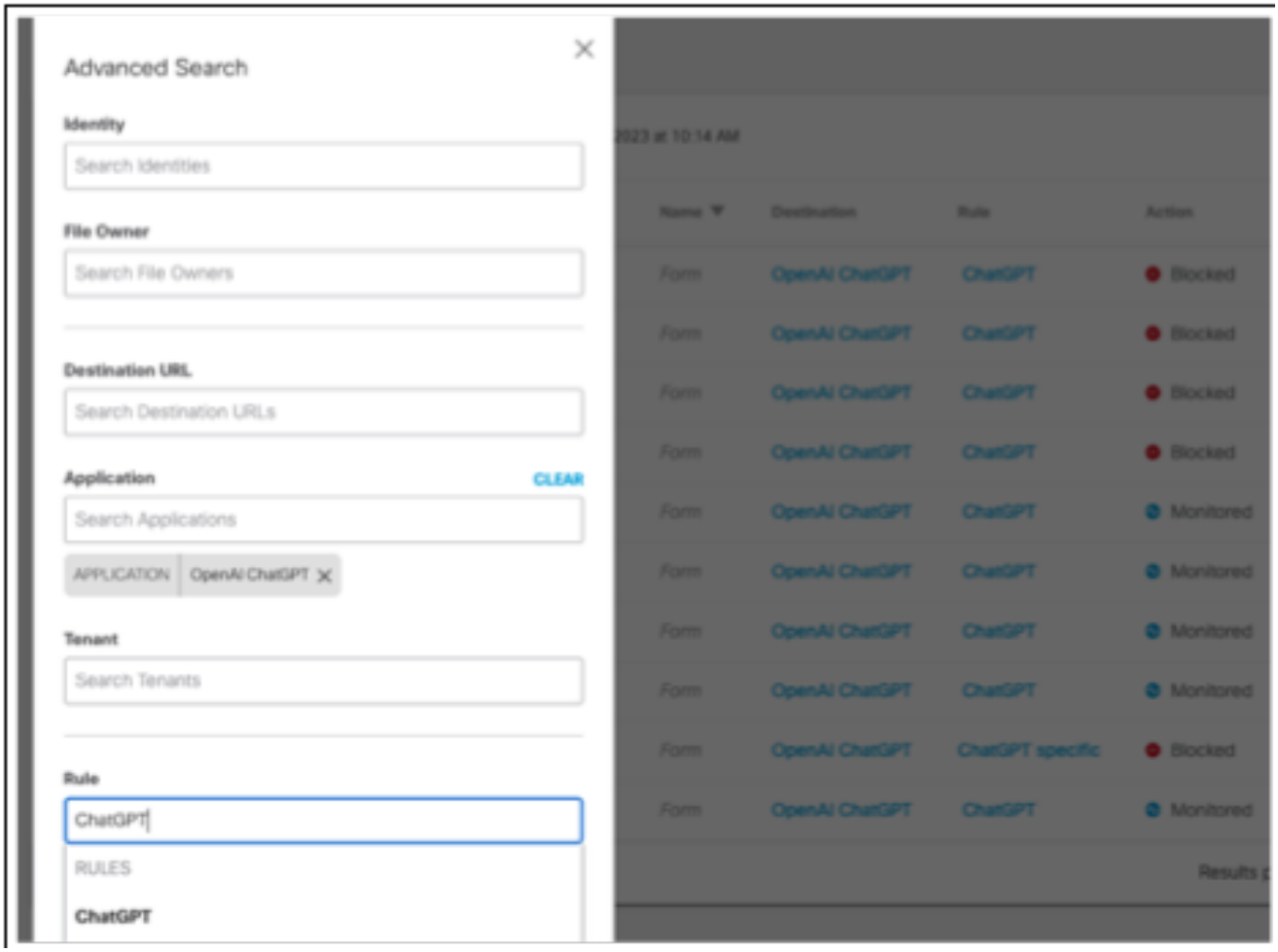
2. **Granular control over ChatGPT access:**
   Customers can now block access to ChatGPT for everyone or allow access only to specific users or groups of users.
   This granular control helps to manage the usage of ChatGPT in line with the security and compliance requirements. Blocking is possible via both DNS and Web policies by selecting *openAI ChatGPT* within Application Settings.




*16221268217748*

3. **Assessing ChatGPT usage risk with DLP:**
   Real Time DLP now enables customers to monitor the type of sensitive information being sent and shared with ChatGPT. This helps to assess the risk associated with ChatGPT usage and take appropriate measures to mitigate potential data leaks or breaches.
   To enable DLP monitoring for ChatGPT, customers can either utilize Real Time rules with the destination set to *All Destinations* or choose *openAI ChatGPT* specifically from the list of available

applications.




*16221283948052*

4. **Allowing safe usage of ChatGPT with DLP:**
   By using our DLP solution, customers can now block prompts to ChatGPT that contain sensitive information. This ensures that employees can continue to use ChatGPT safely and securely, without exposing the organization to potential risks.
   To enable DLP blocking for ChatGPT, customers can either utilize Real Time rules with the destination set to *All Destinations* or choose *openAI ChatGPT* specifically from the list of available applications.


*16221311959572*

5. **Preventing source code leakage to ChatGPT with DLP:**
   With a new *source code* data identifier, customers can use DLP to keep an eye on and stop source code sharing with ChatGPT, safeguarding their valuable intellectual property (IP).

6. **NEW Generative AI application category:**
   *A* new *Generative AI* application category was introduced to tackle usage discovery and prevention for a broader range of tools.