Troubleshoot Umbrella SWG: Policy Debug and Diagnostic Tests

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Overview

Policy Debug Page

Providing a HAR file capture

AnyConnect SWG Logs

Downloading the SWG Diagnostic Tool

Introduction

This document describes how to troubleshoot Umbrella Secure Web Gateway (SWG) with policy debug and diagnostic tests.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Umbrella Secure Web Gateway (SWG).

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

The existing version of the Umbrella Diagnostic Tool provides important information for troubleshooting network identities, Virtual Appliances and AD Integration, and some Roaming Client instances (and can be found here: Umbrella Diagnostic Tool: What to Provide Support When Asked. For users wanting to troubleshoot issues with Secure Web Gateway (SWG), you can use the policy-debug page and the new SWG Diagnostic Tool listed in this article.

Policy Debug Page

As a first step to troubleshooting, go topolicy-debug.checkumbrella.com(or SSE: policy.test.sse.cisco.com) while you are using SWG with the expected Web Policy applied:



You are protected by Cisco Umbrella!

This is a designated test site to easily find which policy you are currently being governed by.
Below is a link to this machine's active internet security policy.

› https://dashboard.umbrella.com/o/1912899/#/configuration/policy/382835

If you are not the Network Administrator, please send a copy of the above link to your Network Administrator.

Diagnostic Info –

General

Org ID:	1912899
Bundle ID:	382835
Origin ID:	44378947
Host:	97eabc3a-80e9-7743-035f-918eae49b5cf.43d7465d.id.opendns.com
Internal IP (public):	128.107.241.182
Timestamp:	Thu, 4 Jun 2020 22:00:34.480274 UTC

Headers

Accept:	text/html, */*; q=0.01
Accept-Encoding:	gzip, deflate
Accept-Language:	en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7,ja;q=0.6,zh-CN;q=0.5
Connection:	keep-alive
Origin:	http://policy-debug.checkumbrella.com
Referer:	http://policy-debug.checkumbrella.com/
User-Agent:	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36

Copy results Download results

360058910251

You can expand **Diagnostic Info**

to view your results. Copy and paste these results to your ticket when submitting your question or replying to your case.

Providing a HAR file capture

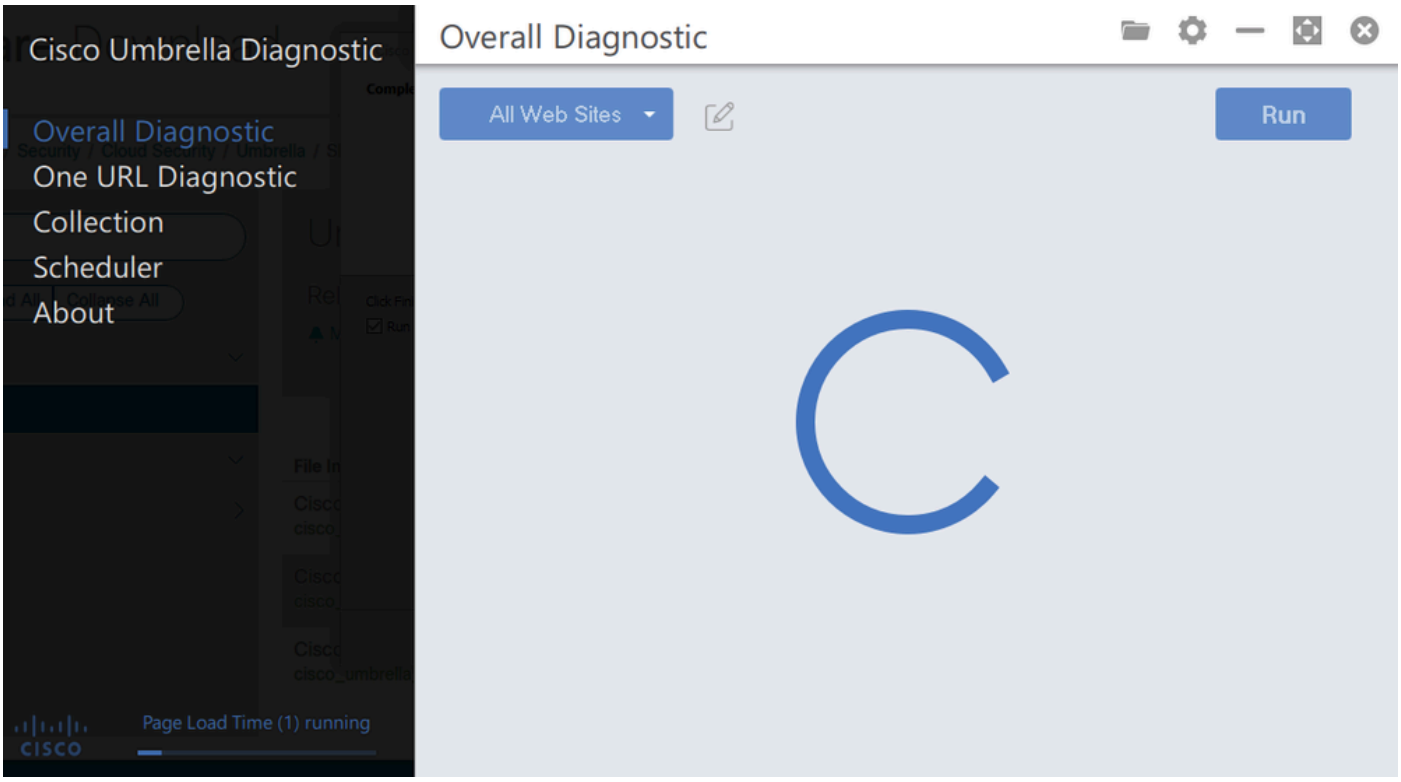
When asked for a HAR capture, see our guide for how to get .HAR files for troubleshooting.

AnyConnect SWG Logs

Capture a DART file. If asked for max logging - see Enable Maximum Debug Logging on AnyConnect SWG Module .Once set, reproduce and then capture a DART.

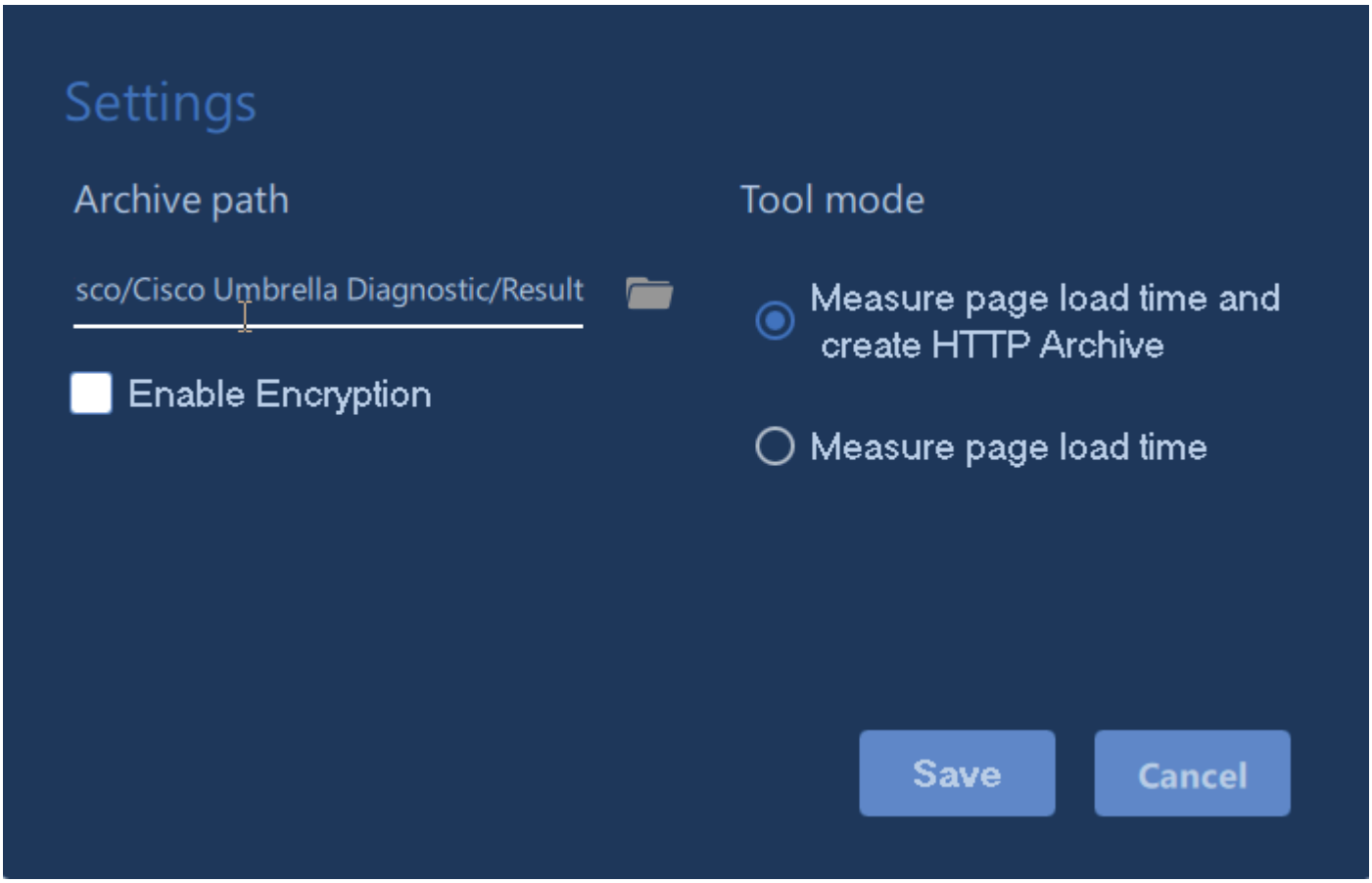
Downloading the SWG Diagnostic Tool

In addition to the above, support can ask for the results of an SWG Diagnostic Tool to provide additional information. The tool is available from software.cisco.com.



360084660592

When you are asked to run the SWG Diagnostic Tool by umbrella support, change the default configuration before proceeding with tests. Select the **Settings** icon and select **Measure page load time and create HTTP Archive**.



360084738691

The SWG diagnostic tool contains these features:

- **Overall Diagnostic:** Compares page load time for one or more websites. A number of popular websites are tested by default. The tool attempts to compare performance with SWG vs Direct Internet Access.
- **One URL Diagnostic:** Test page load time for a single URL. The tool attempts to compare performance via SWG vs Direct Internet Access.
- **Collection:** System configuration information and basic connectivity tests .
- **Scheduler:** The diagnostic tool can be (optionally) configured to run at a scheduled time.

After running the Diagnostic please gather the Results .zip file from the **Archive** folder and upload this to your Umbrella technical support ticket.