# **Collect Packet Capture from MTR Registered Endpoint**

### Contents

Introduction	
<u>Prerequisites</u>	
Components Used	
Background	
<u>Configure</u>	

### Introduction

This document describes how to collect a packet capture from a Cisco Microsoft Teams Room (MTR) device.

### Prerequisites

• Knowledge of onboarding Cisco endpoints to MTR.

### **Components Used**

The information in this document is based on these software and hardware versions:

• Cisco Codec Pro version RoomOS11.7.1.8, fully onboarded into Microsoft Teams as an MTR device. (Or dual registered with Webex Control hub)

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.

### Background

When a Cisco endpoint is onboarded to Microsoft Teams, the ability to capture network traces from the **Issues and Diagnostics > System Logs** menu has been intentionally disabled. It is still possible to collect network traces by using the **Developer API** in the graphical user interface (GUI) if only registered to MS Teams, or using command line of the endpoint when it is dual registered with Microsoft and Webex Control Hub.



**Note**: You must have the admin password that was generated or created during the onboarding process if only performing Microsoft registration. This password is created while using the MTR wizard and offers you the chance to change it at that time.

@ Settings		U	
요 Users			
Security	Execute	In the field below you can enter API commands (xCommand and xConfiguration) directly.	
CUSTOMIZATION	Configurations	Example command:	
X Developer API		xCommand Dial Number: "person∯example.com" Protocol; Sip	
·		Enter commands	
SYSTEM MAINTENANCE			
G Software			
<ol> <li>A source and Diagnostics</li> <li>Backup and Recovery</li> </ol>			
Obtable			
		Evenue -	
		LADUID	

## Configure

Start the capture:

xcommand logging extendedlogging start packetdump:<PICK ONE> PacketDumpRotateSize:<PICK ONE>

(options are full, fullrotate, limited)

Examples:

**xcommand logging extendedlogging start packetdump:full** < captures everything for 3 minutes.

**xcommand logging extendedlogging start packetdump:limited** < captures limited data. Does not capture any real-time transport protocol (RTP).

**xcommand logging extendedlogging start packetdump:fullrotate** < captures everything for up to one hour, 12MB each only keeping last 2 pcap files.

**xcommand logging extendedlogging start packetdump:fullrotate packetdumprotatesize:Large** < captures everything up to 1 hour, 150MB each, and keeps last 2 pcaps only.

Stop the capture:

#### xcommand logging extendedlogging stop

(This is not necessary for Full or Limited captures, but fullrotate runs for one hour unless stopped)

Collect the traces:

Log into the GUI of the codec, or collect from Control Hub, and find the packet capture in the **Run** folder.

ssues a	nd Diagnost	ics	
∽ Issues	System Logs	𝔅 Call Logs	C User Interface Screensho
System L	ogs		
A full archi	ve of the logs on the d	evice is useful for dia	agnosing problems.
This archiv configurati	e includes all current a on, system status, pac	nd historical logs, in ket captures and dia	addition to current system gnostics information.
Download	i logs 🔻		
Download Full log	s (recommended) at		

System Logs Menu