



Cisco AI Assistant for Support

<https://supportassistant.cisco.com/>

Cisco Customer Experience
September 2025



Agenda



Introduction



How to access?



Conversations



Help, Commands & Feedback

What is it?

Cisco AI Assistant for Support offers customers and partners a self-service experience for common case, bug, RMA inquiries and basic transactions. It even can connect customers with case owners, managers and TAC duty managers.

Benefits

- Easy to access
- Easy to use
- Seamlessly connect to an Engineer
- No need to call 1-800



Customers
and
Partners

Ask a Question
←
→
Get a Response



Cisco AI Assistant
for Support

Self-Service Experience for TAC Engagements

Get Things Done Quicker Without Waiting in Queue

Get status

Case, Bug, RMA

Update

Update case, Upload files and Request update

Subscribe

Case summary updates, case severity, status changes, Proactive TAC Alerts

Connect

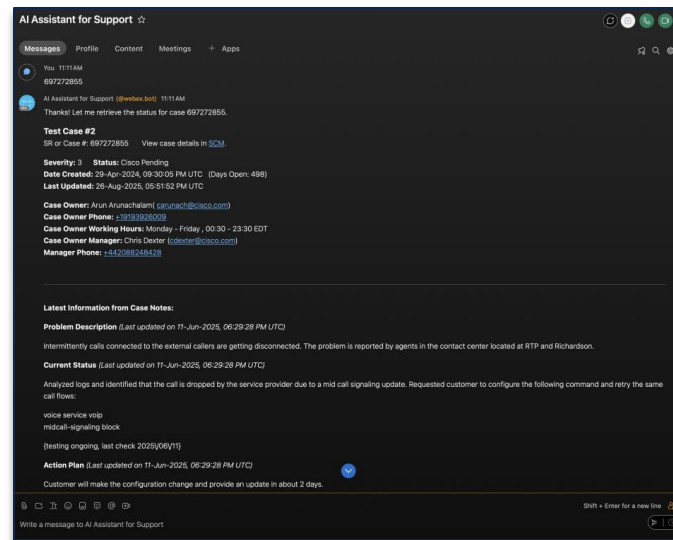
Engineer via Virtual Spaces, Virtual Meeting or Phone Callback

Initiate

Reassign, Schedule dispatch, Raise severity, Escalation, Close case, Add Contract

Be Proactive

Proactive TAC Alerts, Bug Applicability Checks & IOS XE SW Hardening Assessments



Natural language and text commands

*Cisco AI Assistant for Support was formerly known as
“Cisco Support Assistant” and “TAC Connect Bot”.
The screenshots in this slide deck may reference former names.*

How to access?



Multiple ways to interact with the Assistant

<https://supportassistant.cisco.com>

Support Case Manager

Virtual Spaces

Cisco AI Assistant for Support

Self-serve experience for TAC Engagements. Get things done quicker without waiting in queues.

Cisco AI Assistant for Support: At-a-Glance

Get Started

- Chat right here
- Chat in Webex App
- CSA Extension

Actions	Case	Created	Sev	Status	Title
☆	Hello! I can help you get case, bug, RMA details and connect with Cisco TAC. d assist				
☆	697959220	09/13/2024	3	Cisco Pending	Need help v

Hello! I can help you get case, bug, RMA details and connect with Cisco TAC.

AI Assistant for Support 8/14/25, 12:01 PM

Hello! I can help you get case details and connect with Cisco TAC. You can make the following requests in English language:

- @Support what is the status
- @Support change status to cisco pending
- @Support add participant (email address)
- @Support connect with engineer
- @Support create a virtual space
- @Support request an update
- @Support update the case
- @Support escalate
- @Support raise severity
- @Support requeue
- @Support close the case

I can help you manage cases that are opened from [Cisco.com Support Case Manager](#). Currently, I can't open new cases or answer technical questions. Type **/list commands** to get a list of command requests and find details of supported features using the [documentation](#) and [demo videos](#).

Use @(AI Assistant for Support) to interact with the assistant in virtual spaces created in the context of a case

How to **escalate** a technical support case

If you have opened a service request and are not satisfied with the progress, use the following procedure to escalate and connect directly to a resolution owner



- ▶ Escalate using **Cisco AI Assistant for Support** at <https://supportassistant.cisco.com/escalate>, via Webex App, on [Support Case Manager](#) or Virtual Spaces
- ▶ Enter case number
- ▶ Provide escalation reason
- ▶ Choose “Escalate to TAC Manager”
- ▶ Provide phone number for S1/S2 case or email address for S3/4 case

Severity Definitions

Severity 1

Critical impact on business operations. Cisco hardware, software, or as-a-service product is down.

Severity 2

Substantial impact on business operations. Cisco hardware, software, or as-a-service product is degraded.

Severity 3

Minimal impact on business operations. Cisco hardware, software or as a service product is partially degraded.

Severity 4

No impact on business operations. Features, implementation, or configuration assistance.

Demo


[YouTube](#)




Support Case Manager




Start the interaction in the context of a case

 Cisco AI Assistant for Support
Knowledge Scope: Cases, Bugs and RMA Management

 Hi there! I am Cisco AI Assistant for Support.

16:46:46




I can help you get case, bug, RMA details and connect with Cisco TAC. You can converse with me in English language or use commands. Simply enter the case number as shown in the examples below and get the latest case summary.

612345678 - Cisco TAC case
00123456 - Duo support case
12345678 - Meraki support case
S-CS-0001234 - ThousandEyes support case



I can perform software hardening assessment for your IOS XE devices. Currently I can't open new cases or answer technical question.

[Common Tasks](#) [List Commands](#) [Documentation](#) [Demo Video](#)

16:46:46









To ask questions and perform tasks in additional domains, please interact with me at the following places:



-  Licensing
-  Webex Q&A and Tasks

16:46:46

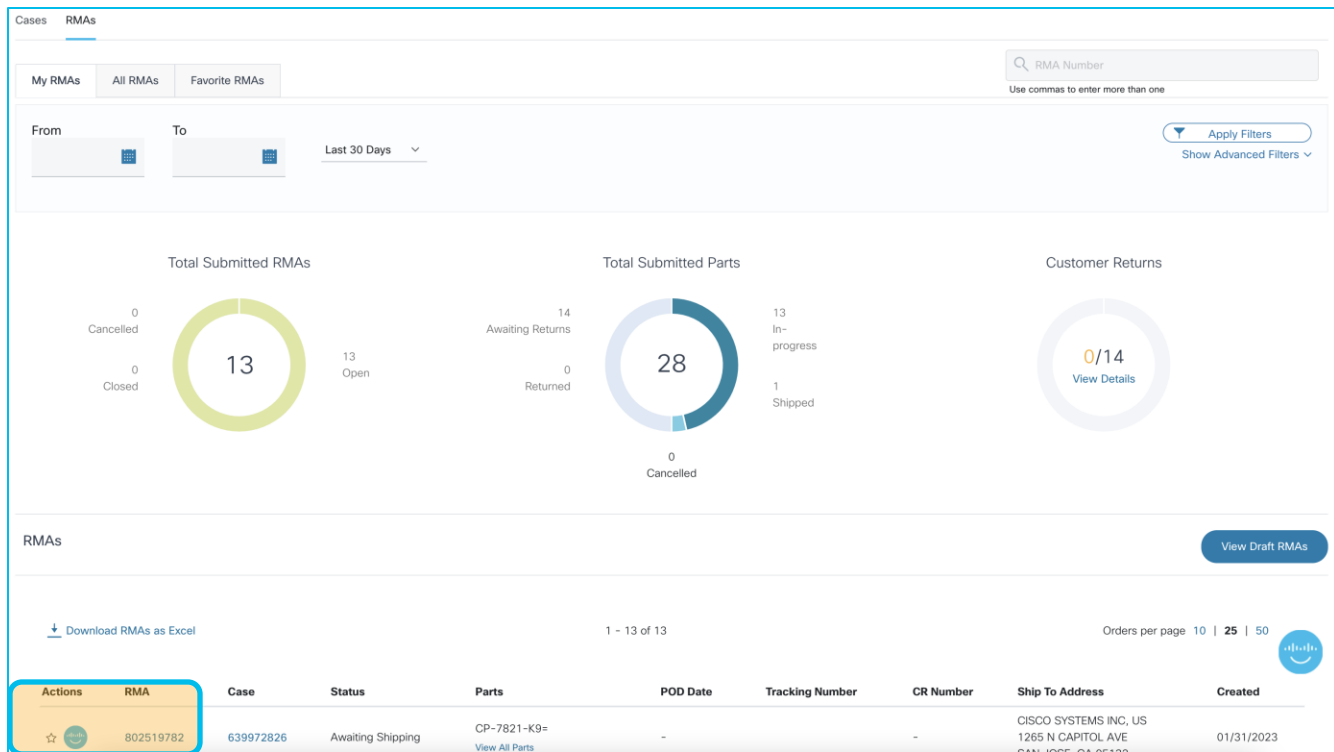
Enter message (Use Shift + Enter to add a new line)

Rate your experience  

 Proactive TAC Alerts  Chat in Webex  Start Over  Help

 Release Notes  Docs and Videos

Start the interaction in the context of a RMA



“Floating icon” – Start the interaction!

Support Case Manager

Create and manage Support cases for Arun Arunachalam (carunach@cisco.com) ▼

Open New Case ▼

Cases RMA's

My Cases All Cases Favorites

Case or Customer Reference Number


Use commas to enter more than one


Show ☒ Open Cases ☒ Draft Cases ☐ Closed Cases ☒ Created ☐ Updated Last 30 Days ▼

Apply Filters

Show Advanced Filters ▼

Download Cases as Excel 1 - 1 of 1 Cases per page: 10 | 25 | 50

Ask the bot	Case	Created ▼	Sev	Status	Summary
☆ 	693956300	01/31/2023	3	Cisco Pending	DNS DDoS Proactive Detection (Test case)



Chat in Webex

The screenshot displays the Cisco AI Assistant interface. At the top, the header reads "Cisco AI Assistant for Support" with the subtitle "Knowledge Scope: Cases, Bugs and RMA Management". The chat history shows three messages from the assistant, each preceded by a timestamp (16:41:07, 16:41:07, and 16:41:14). The assistant's responses are: "Test case", "Let me check for Proactive TAC Alerts in the context of this case. This may take a few seconds.", and "All good! There are no critical bugs or top trending issues that you need to be aware of in the context of this case." Below the chat history, a section titled "Actions available for case 693098774 :" lists eight actions in a grid: "Add Case Notes", "Request New Update", "Close Case", "Raise Case Severity", "Request New Engineer", "Escalate Case", "Case Feedback", and "Mark Case As Favorite". A "Show more Actions" link is located below the grid. At the bottom of the interface, there is a text input field with the placeholder "Enter message (Use Shift + Enter to add a new line)". To the left of the input field is a "Rate your experience" section with icons for thumbs up and down, and a "Proactive TAC Alerts" notification. To the right of the input field are icons for "Chat in Webex", "Start Over", and "Help". A blue callout box with a white border points to the "Chat in Webex" icon, containing the text "Click to create a 1:1 space with the assistant." The bottom right corner of the interface shows a "Release Notes" link and a "Docs and Videos" link.

Chat in Webex

1:1 Webex Space Created

×

To start interacting with the bot, login to the Webex app using one of the options below with your carunach@cisco.com account:

Note: Interaction with Cisco AI Assistant for Support using Webex App is currently done using tac.connect@webex.bot.

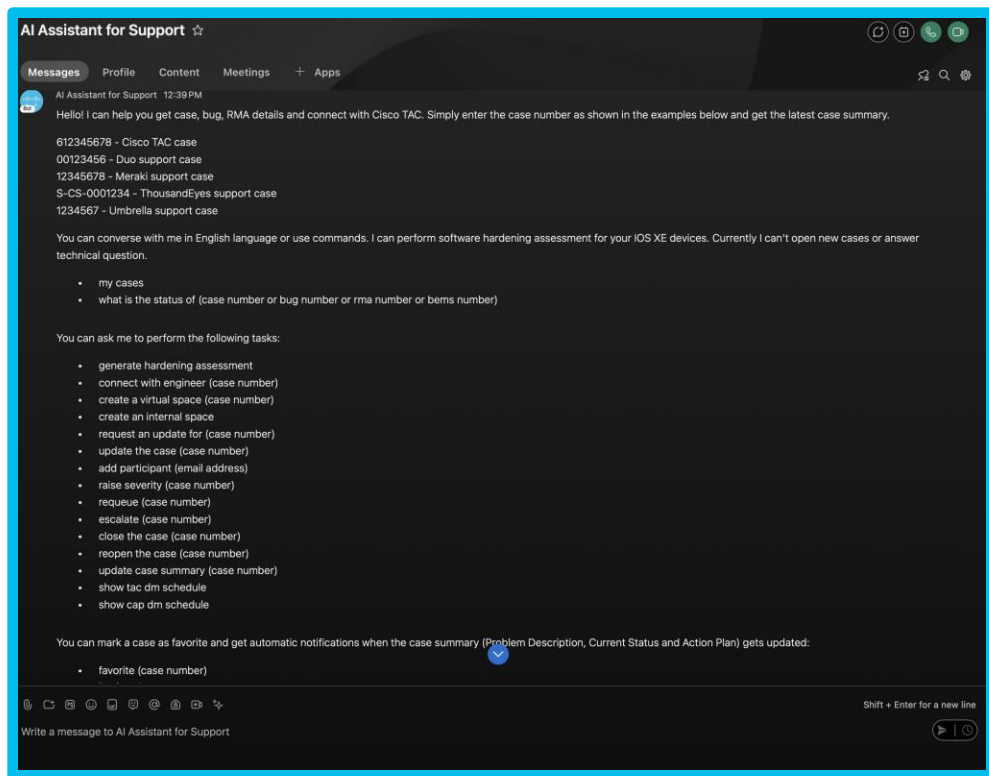
Webex
Desktop App

OR

Webex
Web Client

You can download the app [here](#).

Welcome Message Has Everything to Get Started



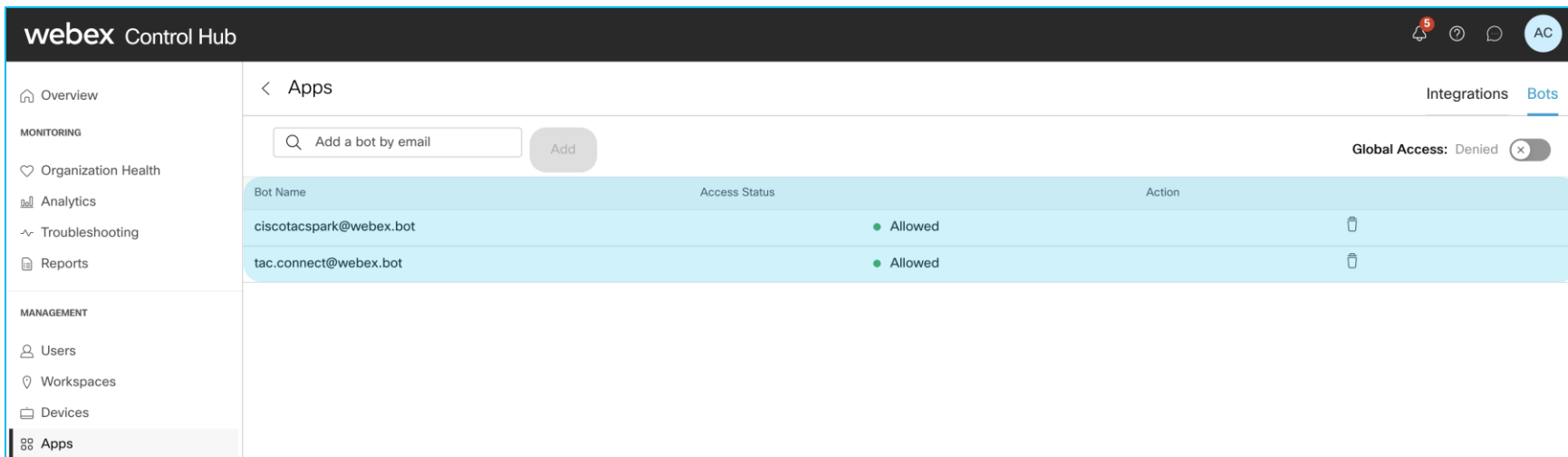
Webex Interface



Prerequisite

- **What** – The email address that is used to login to Webex **MUST** be the primary email address associated with your Cisco.com profile.
https://rpfa.cloudapps.cisco.com/rpfa/profile/profile_management.do
- **Why** – To protect customer data.
- **How** – The email address of Webex user account is mapped to Cisco.com user-id. This user-id is used to authorize case, bug and RMA data access.

Prerequisite



The screenshot shows the Webex Control Hub interface. The left sidebar contains navigation links for Overview, MONITORING (Organization Health, Analytics, Troubleshooting, Reports), and MANAGEMENT (Users, Workspaces, Devices, Apps). The main content area is titled 'Apps' and includes a search bar 'Add a bot by email' and an 'Add' button. A table lists the bots and their access status:

Bot Name	Access Status	Action
ciscotacspark@webex.bot	Allowed	
tac.connect@webex.bot	Allowed	

Global Access: Denied

If access to bot is disabled in your Webex site, please allow access to tac.connect@webex.bot and ciscotacspark@webex.bot for Cisco TAC interactions.

Steps to Get Started

- Login to <https://supportassistant.cisco.com/>.
- Click “Chat in Webex App” button.
- You will be invited to a 1:1 Virtual space. That’s it!

Note: The email address associated with your Cisco.com user ID will be used to create the 1:1 Webex space.

Steps to Get Started

1

Cisco AI Assistant for Support

Self-serve experience for TAC Engagements. Get things done quicker without waiting in queues.

[Cisco AI Assistant for Support: At-a-Glance](#)

Get Started

- Chat right here
- Chat in Webex App
- CSA Extension

2

Setting-up a 1:1 Webex Space with carunach@cisco.com

3

1:1 Webex Space Created

To start interacting with the bot, login to the Webex app using one of the options below with your carunach@cisco.com account:

Note: Interaction with Cisco Support Assistant using Webex App is currently done using tac.connect@webex.bot.

Webex Desktop App

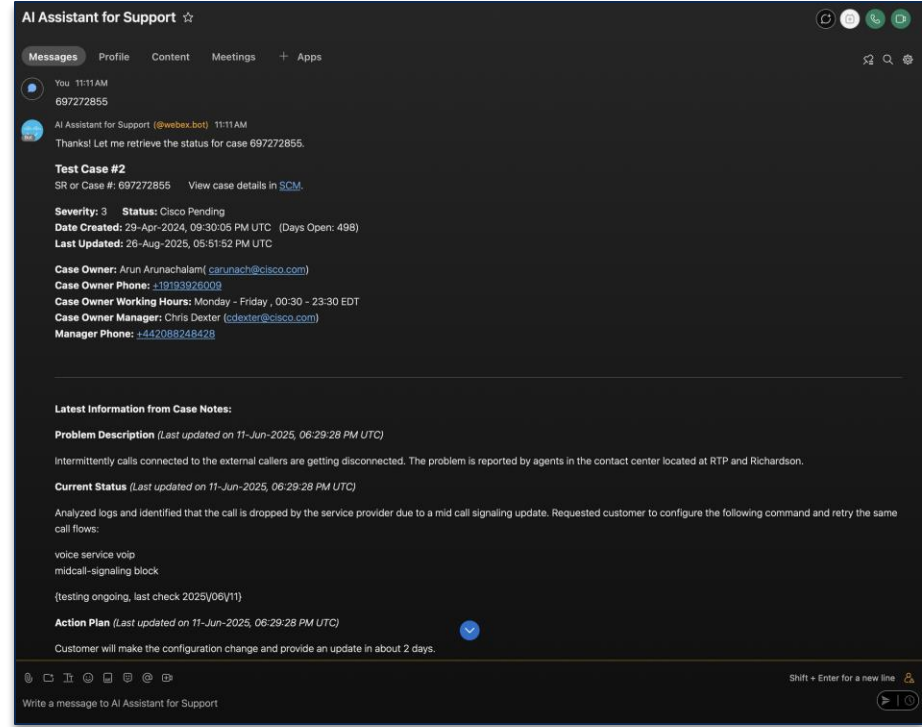
OR

Webex Web Client

You can download the app [here](#).

Sample Questions

- who are you
- what is the status of 689644400
- status CSCtz27004
- 88238608
- /help
- connect me to engineer
- /feedback <message>



Web Interface

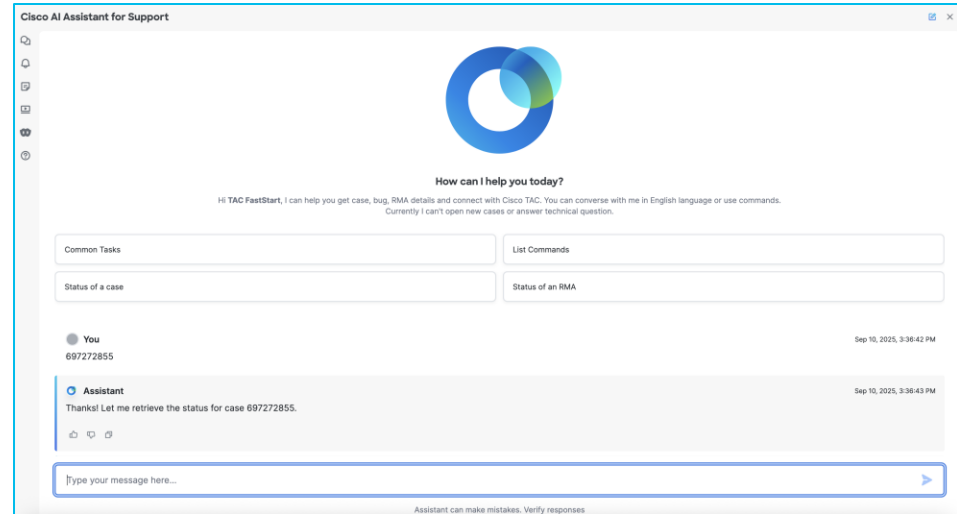


Steps to Get Started

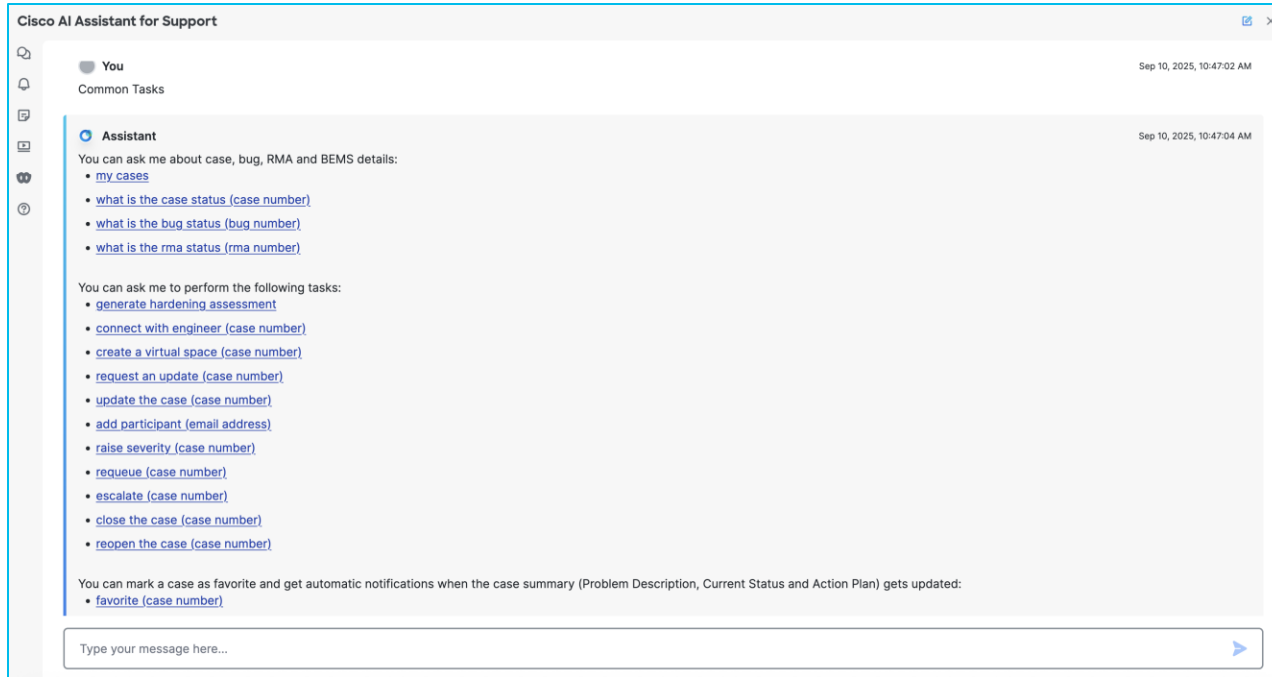
- Login to <https://supportassistant.cisco.com/>
- Click “Chat right here” button.

Sample Questions

- who are you
- what is the status of 690833877
- status CSCtz27004
- 88238608
- /help
- connect me to engineer
- /feedback <message>



Enhanced Web Interface with Clickable Intents




Conversations: Status view and Case Updates




Prioritized View of Your Cases

my cases



Thanks! Let me retrieve the cases for user ID tacfaststart@gmail.com



Cases that need my attention

1. (S3, 09/10/2022) [693098774](#) - CUBE SIP Profiles

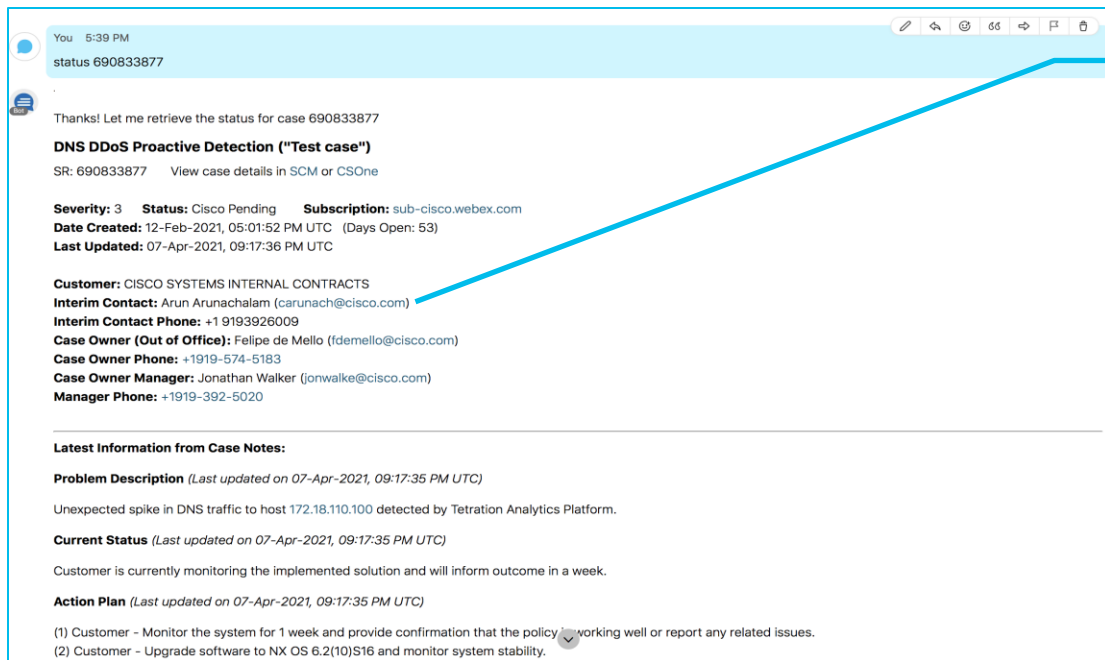
Cisco pending cases

1. (S3, 10/25/2022) [690790352](#) - Need UCS server replacement
2. (S3, 01/24/2023) [690223946](#) - CUBE - Intermittent call disconnects
3. (S3, 01/31/2023) [690774441](#) - SDWAN Test Case

Cases that needs my confirmation to close

1. (S3, 10/11/2022) [692164600](#) - Need help with SIP profile troubleshooting.

Get Case Status: Case Summary



You 5:39 PM
status 690833877

Thanks! Let me retrieve the status for case 690833877

DNS DDoS Proactive Detection ("Test case")
SR: 690833877 View case details in SCM or CSOne

Severity: 3 **Status:** Cisco Pending **Subscription:** sub-cisco.webex.com
Date Created: 12-Feb-2021, 05:01:52 PM UTC (Days Open: 53)
Last Updated: 07-Apr-2021, 09:17:36 PM UTC

Customer: CISCO SYSTEMS INTERNAL CONTRACTS
Interim Contact: Arun Arunachalam (carunach@cisco.com)
Interim Contact Phone: +1 9193926009
Case Owner (Out of Office): Felipe de Mello (fdemello@cisco.com)
Case Owner Phone: +1919-574-5183
Case Owner Manager: Jonathan Walker (jonwalke@cisco.com)
Manager Phone: +1919-392-5020

Latest Information from Case Notes:

Problem Description (Last updated on 07-Apr-2021, 09:17:35 PM UTC)
Unexpected spike in DNS traffic to host 172.18.110.100 detected by Tetration Analytics Platform.

Current Status (Last updated on 07-Apr-2021, 09:17:35 PM UTC)
Customer is currently monitoring the implemented solution and will inform outcome in a week.

Action Plan (Last updated on 07-Apr-2021, 09:17:35 PM UTC)
(1) Customer - Monitor the system for 1 week and provide confirmation that the policy is working well or report any related issues.
(2) Customer - Upgrade software to NX OS 6.2(10)S16 and monitor system stability.

Interim contact is displayed if the case owner is out of the office.

Note: External users can access the case data only if there are authorized. This requires the user to have the service contract used to open the case to be associated with their Cisco.com profile.

Adding the user's email address in the CC Recipients field at the time of case open in Support Case Manager does not enable case data access.

Get Case Status: Proactive TAC Alerts

Device specific S1 and S2 Bugs detected from log files attached to the case
(Experimental feature: Available for IOS XE, UCS, ASA, ISE WLC, NXOS, VCS-C, VCS-E, Jabber, UCCE)

Let me check for Proactive TAC Alerts in the context of this case. This may take a few seconds.

Proactive TAC Alerts

Critical Issues (Applicable to devices in your network. Please consult with your partner or Cisco professional services teams as needed.)

- [CSCvr93800](#)

[C240M5]:- Kernel panic error due to snmp-subagentd during stress



Device ID: ABC12345678

Issue detected on: 29-Sep-2022, 04:04:33 PM UTC

Trending Issues (Currently observed in the field)

- [Field Notice: FN - 70432](#)

Improved Memory RAS Features for UCS M5 Platforms - Software Upgrade Recommended



- [Field Notice: FN - 70595](#)

UCS Servers Might Fail to Boot if Memory Errors Occur During Boot - Software Upgrade Recommended



- [Field Notice: FN - 72301](#)

M5 Server BIOS POST Hang With 2x Memory Refresh Rate - BIOS/Firmware Upgrade Recommended



- [Field Notice: FN - 70545](#)

SSD Will Fail at 40,000 Power-On Hours - BIOS/Firmware Upgrade Recommended



Enter message (Use Shift + Enter to add a new line)



Rate your experience 😊 😞



Release Notes

Docs and Videos

Chat in Webex

Start Over

Help

Get Case Status: Proactive TAC Alerts

Recent High Impact issues observed in the Field and relevant to the product / solution handled in the case

The screenshot shows a chat window with a header bar containing the case title 'midcall-signaling block'. Below the header, a message from the support agent states: 'Let me check for Proactive TAC Alerts in the context of this case. This may take a few seconds.' The main content area is titled 'Proactive TAC Alerts' and contains three sections: 'Trending Issues (Currently observed in the field)', 'Tool updates', and 'Articles and Bulletin updates'. The 'Trending Issues' section is highlighted with a blue border and contains two items: 'CSOvz89043' with the description 'Prevent SIP services from being blocked even if license usage ACK was not received' and 'FN - 72323' with the description 'Cisco IOS XE Software: QuoVadis Root CA 2 Decommission Might Affect Smart Licensing, Smart Call Home'. The 'Tool updates' section contains one item: 'Log Advisor for CUBE' with the description 'Learn about Log collection best practices for common troubleshooting scenarios'. The 'Articles and Bulletin updates' section contains one item: 'End of Support for the H.323 call control features in Cisco IOS XE Software' with the description 'Cisco IOS XE 17.5 release will be the last to provide support for H.323 features'. At the bottom of the chat window, there is a text input field with the placeholder 'Enter message (Use Shift + Enter to add a new line)', a 'Rate your experience' section with smiley face icons, and a footer bar with links for 'Release Notes', 'Docs and Videos', 'Chat in Webex', 'Start Over', and 'Help'.

midcall-signaling block

Let me check for Proactive TAC Alerts in the context of this case. This may take a few seconds.

Proactive TAC Alerts

Trending Issues *(Currently observed in the field)*

- **CSOvz89043**
Prevent SIP services from being blocked even if license usage ACK was not received
- **FN - 72323**
Cisco IOS XE Software: QuoVadis Root CA 2 Decommission Might Affect Smart Licensing, Smart Call Home

Tool updates

- **Log Advisor for CUBE**
Learn about Log collection best practices for common troubleshooting scenarios

Articles and Bulletin updates

- **End of Support for the H.323 call control features in Cisco IOS XE Software**
Cisco IOS XE 17.5 release will be the last to provide support for H.323 features

Enter message (Use Shift + Enter to add a new line)

Rate your experience

Release Notes Docs and Videos Chat in Webex Start Over Help

Get Case Status: Proactive TAC Alerts

Recent Tool updates that are relevant to the product / solution handled in the case

The screenshot shows a chat window with a header bar containing the case title 'midcall-signaling block'. Below the header, a message from the support agent states: 'Let me check for Proactive TAC Alerts in the context of this case. This may take a few seconds.' The main content area is titled 'Proactive TAC Alerts' and lists several items:

- Trending Issues** (Currently observed in the field)
 - CSCvz89043**: Prevent SIP services from being blocked even if license usage ACK was not received
 - FN - 72323**: Cisco IOS XE Software: QuoVadis Root CA 2 Decommission Might Affect Smart Licensing, Smart Call Home
- Tool updates** (highlighted with a blue border)
 - Log Advisor for CUBE**: Learn about Log collection best practices for common troubleshooting scenarios
- Articles and Bulletin updates**
 - End of Support for the H.323 call control features in Cisco IOS XE Software**: Cisco IOS XE 17.5 release will be the last to provide support for H.323 features

At the bottom of the chat window, there is a text input field with the placeholder 'Enter message (Use Shift + Enter to add a new line)', a 'Rate your experience' section with smiley face icons, and a navigation bar with links for 'Release Notes', 'Docs and Videos', 'Chat in Webex', 'Start Over', and 'Help'.

Get Case Status: Proactive TAC Alerts

Recent Articles and Bulletins that are relevant to the **product / solution** handled in the case

The screenshot shows a chat window with a header bar containing the case title 'midcall-signaling block'. Below the header, a message from the support agent states: 'Let me check for Proactive TAC Alerts in the context of this case. This may take a few seconds.' The main content area is titled 'Proactive TAC Alerts' and is divided into three sections: 'Trending Issues (Currently observed in the field)', 'Tool updates', and 'Articles and Bulletin updates'. The 'Articles and Bulletin updates' section is highlighted with a blue border. At the bottom of the chat window, there is a text input field with the placeholder 'Enter message (Use Shift + Enter to add a new line)', a 'Rate your experience' section with smiley face icons, and a navigation bar with links for 'Release Notes', 'Docs and Videos', 'Chat in Webex', 'Start Over', and 'Help'.

midcall-signaling block

Let me check for Proactive TAC Alerts in the context of this case. This may take a few seconds.

Proactive TAC Alerts

Trending Issues *(Currently observed in the field)*

- [CSCvz89043](#)
Prevent SIP services from being blocked even if license usage ACK was not received |
- [FN - 72323](#)
Cisco IOS XE Software: QuoVadis Root CA 2 Decommission Might Affect Smart Licensing, Smart Call Home |

Tool updates

- [Log Advisor for CUBE](#)
Learn about Log collection best practices for common troubleshooting scenarios |

Articles and Bulletin updates


- [End of Support for the H.323 call control features in Cisco IOS XE Software](#)
Cisco IOS XE 17.5 release will be the last to provide support for H.323 features |

Enter message (Use Shift + Enter to add a new line)

Rate your experience 😊 😞

Release Notes Docs and Videos Chat in Webex Start Over Help

Get Case Status: Contextual Tasks




Customer is installing a new 3-node DNAC cluster in which each node is connected to a separate physical switch. Customers brought down one of the nodes and observed that high availability isn't working.


Current Status *(Last updated on 19-Nov-2020, 04:26:42 PM UTC)*


Worked with the customer and corrected the VLAN configuration to get high availability working.


Action Plan *(Last updated on 19-Nov-2020, 04:21:40 PM UTC)*


Customer will perform additional tests and provide an update on 11/20. After successful confirmation, we can close the case.


 Actions available for case **690329099**:



Add case notes



Request update



Close case



Raise Case Severity



Request New Engineer


Escalate case


Mark case as favorite


Case Feedback



Connect to Engineer



Create Space


Hide Actions ^


Enter message (Use Shift + Enter to add a new line)


Rate your experience 😊 😞

 Release Notes

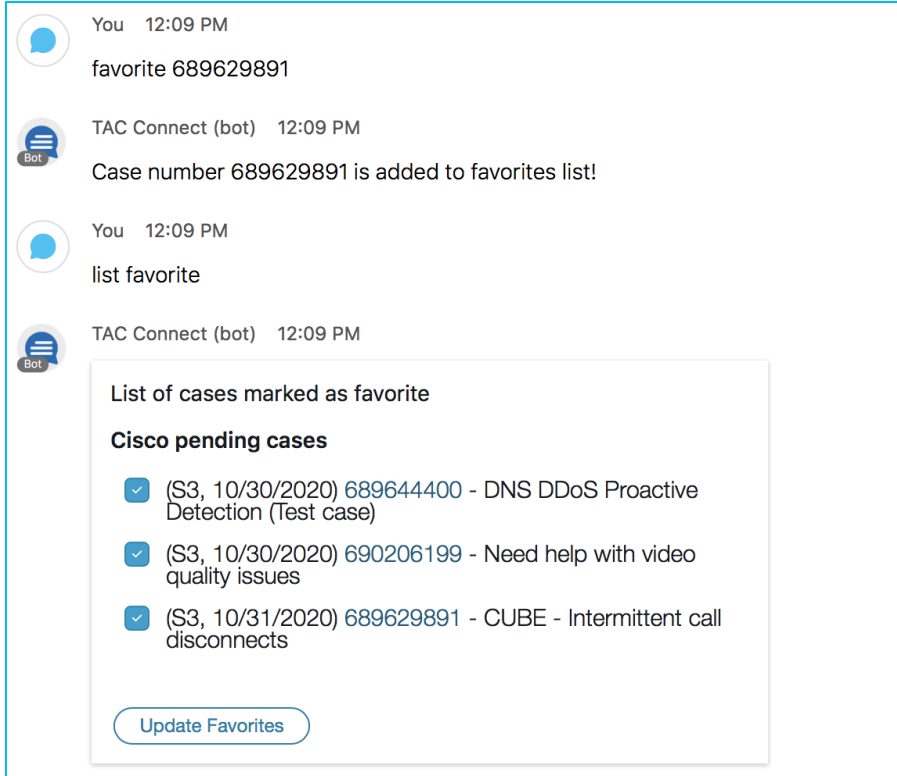
 Docs and Videos

 Chat in Webex

 Start Over

 Help

Mark Cases as Favorite



The screenshot shows a chat interface with a blue border. It contains four messages:

- You** 12:09 PM: favorite 689629891
- TAC Connect (bot)** 12:09 PM: Case number 689629891 is added to favorites list!
- You** 12:09 PM: list favorite
- TAC Connect (bot)** 12:09 PM: A white box containing:
 - List of cases marked as favorite
 - Cisco pending cases**
 - Three items, each with a blue checkmark icon:
 - (S3, 10/30/2020) 689644400 - DNS DDoS Proactive Detection (Test case)
 - (S3, 10/30/2020) 690206199 - Need help with video quality issues
 - (S3, 10/31/2020) 689629891 - CUBE - Intermittent call disconnects
 - An "Update Favorites" button at the bottom.

Automatic **notifications in Webex App** when

1. Case status changes
2. Case severity changes
3. Problem description, Current Status or Action Plan is updated

Webex App Notifications for Favorite Cases



The status of [690774441](#) - "SDWAN Test Case" was changed from Customer Pending to Cisco Pending. Please use /list favorites to manage your case favorites subscription.

The severity of [690774441](#) - "SDWAN Test Case" was changed from 1 to 3. Please use /list favorites to manage your case favorites subscription.

[690774441](#) - "SDWAN Test Case" has been updated. Please use /list favorites to manage your case summary subscription

Current Status (Last updated on 10-Jun-2023, 9:25:20 PM UTC)

ISR 4451 DNS configuration updated and system is able to communicate with vBond. 10-June-2023.

Get Status of Favorite Cases

Get statuses of **three** recently updated favorite cases through a single request

You 9:04 AM
status favorites

Thanks! Let me retrieve the 3 recently updated favorite case statuses.

DNS DDoS Proactive Detection (Test case)
SR: 689644400 [View case details in SCM](#) or [CSOne](#)

Severity: 3 **Status:** Customer Updated **Subscription:** sub-cisco.webex.com
Date Created: 05-Aug-2020, 09:22:41 PM UTC (Days Open: 54)
Last Updated: 29-Sep-2020, 12:52:35 PM UTC

Customer: Cisco
Case Owner: Chidambaram Arunachalam (carunach@cisco.com)
Case Owner Phone: +19193926009
Case Owner Manager: Marc Holloman (mholloma@cisco.com)
Manager Phone: +19193927144

Linked Bugs:

- [CSCTz27004](#)

Latest Information from Case Notes:


Problem Description (Last updated on 26-Sep-2020, 03:47:42 AM UTC)
Unexpected spike in DNS traffic to host 172.18.110.100 detected by Tetration Analytics Platform. Case was opened proactively to avoid any user impact.

Current Status (Last updated on 13-Sep-2020, 06:32:42 PM UTC)
Issue resolved and monitoring is in progress.

Action Plan (Last updated on 13-Sep-2020, 06:32:42 PM UTC)
(1) Customer - Monitor the system for 1 week and provide confirmation that the policy is working well or report any related issues.
(2) Customer - Upgrade software to NX OS 6.2(10)S16 is scheduled on 9/24, monitor system stability.


Resolution Summary (Last updated on 26-Sep-2020, 03:47:42 AM UTC)
Issue was mitigated by rerouting DNS traffic from 10.x.x.x network to a blackhole and storing 10% in the data collection server. SDN Controller policy to automatically detect

Get Bug Status

 You 8:15 PM

status CSCtz27004

NEW MESSAGES



Thanks! Let me retrieve the status for bug csctz27004

NVRAM correction when bad sectors found.

CSCtz27004

- **Status** : Fixed
- **Product** : Cisco Nexus 7000 Series Switches
- **Severity** : Enhancement(6)
- Click [here](#) to view known affected and fixed releases.

Bug Release-note :

Symptom:
Supervisor-1 may log the following messages and report NVRAM Gold diagnostic failure:


%KERN-2-SYSTEM_MSG: Invalid cksum for block 17 expected 0x304 got 0x384 - kernel
%KERN-0-SYSTEM_MSG: NVRAM Error: (line 464):Invalid cksum for block 17 expected 0x304 got 0x384 - ker

%DEVICE_TEST-STANDBY-2-NVRAM_FAIL: Module 5 has failed test NVRAM 20 times on device NVRAM due to error Bad blocks found on nvram
%DIAGCLIENT-STANDBY-2-EEM_ACTION_HM_SHUTDOWN: Test has been disabled as a part of default EEM action

Conditions:
NVRAM diagnostic test verifies that stored cksum matches the cksum computed for block contents. If there is a mismatch in cksum values, the condition is logged and test will be disabled after multiple consecutive failures.

Workaround:
NVRAM block failure may be a result of a single-event upset / bit-flip (transient condition). Prior to this enhancement, no error-correction is performed and the issue will only be cleared by reload of the affected supervisor.

Details of this enhancement:
This enhancement provides error correction for NVRAM data corruption caused by single-event upsets by replacing corrupted blocks with contents from mirrored copy in DRAM. The NVRAM Gold diagnostic will continue to log the initial checksum failure, but will perform a block rewrite that will prevent further test iterations from failing.



If multiple test failures occur for the same NVRAM block, a hard-failure may have occurred and a TAC case should be opened for RMA.

Get RMA Status

You 10:36 AM
801152201

Thanks! Let me retrieve the status for RMA 801152201

RMA 801152201: Service Order RMA API

- **Status:** Booked
- **Case Number:** 689928867
- **Order Date:** 2020-09-17
- **Requested Ship Date:** 2020-09-17
- Visit the [Product Returns and Replacement](#) page to view the shipment, tracking and return details

Acknowledgment Contact:
Shikha Saun
ssaun@cisco.com
918067336057

Ship To Contact:
Darin Collins
darcolli@cisco.com
12145575918

Shipping address:
Darin Collins
CISCO SYSTEMS
2450 E PRESIDENT GEORGE BUSH HWY
RCDN9
RICHARDSON
TX
UNITED STATES

Tracking Details:
Tracking number: 1699394
Courier: Flash Logistics
Ship date: 2020-09-17


[Tracking URL \(Google Search\)](#)

Field Engineer details
are included here if
available.

Track RMA Shipment
using Search URL
and Tracking number

Get RMA Return Status

return status 802294873

 **RMA 802294873**


- **Status:** Closed
- **Case Number:** 693725859
- **Order Date:** 2022-06-10
- Visit the [Product Returns and Replacement](#) page to view the shipment, tracking and return details

Received Return Parts:

1. Part# abc12345678 (ISR4451-X-AX/K9 received on 2022-06-15 12:09:14 UTC)

Return Parts Details

return status 802530052

 **RMA 802530052**

- **Status:** Booked
- **Case Number:** 694407555
- **Order Date:** 2022-10-13
- Visit the [Product Returns and Replacement](#) page to view the shipment, tracking and return details

Pending Return Parts:

Please return the following parts to Cisco by the given date. Use the [Product Online Web Returns Tool](#) to schedule pickups of parts for return to Cisco, and print shipping labels.

1. abc12345677 (ISR4451-X-AX/K9 by 2022-10-23 13:36:34 UTC)

© 2025 Cisco and/or its affiliates. All rights reserved.

Update a Case

update case 689644400



Please enter the note details for the case 689644400 (DNS DDoS Proactive Detection (Test case)).

The problem reoccurred today and we have attached the logs

Submit


Cancel Request

Note: Use the [Support Case Manager](#) tool to upload files to the case. Alternate methods are described [here](#).





Thanks! Successfully added the note to the case 689644400

Update a Case and Upload Files in Webex App


 You 1:38 PM

update case


 Would you like to use the case number 690833877? Please enter 'Yes' to use this case number or provide another case number.


 You 1:38 PM

yes


 Please enter the note details and upload files for the case 690833877 (DNS DDoS Proactive Detection ("Test case")). If you would like to update a different case, please enter a new case number.

Privacy notice: As a user of this collaboration space you are in control of your data in this space and have the option to delete any of the data uploaded into the space. For more information, please visit the [WebEx Help Center](#).

 You 1:40 PM



Uploading requested file

 Thanks! Successfully added the note to the case 690833877. Please wait while I upload the file.

File 686911421-cognitive-book-external.pdf uploaded successfully.

Add Participants to CC-list of the Case



You 9:09 PM

/add-participant ic2user4@gmail.com



Would you like to use the case number 689644400? Please enter 'Yes' to use this case number or provide another case number.



You 9:09 PM


yes



Sure. Let me check whether the participant can be added.

ic2user4@gmail.com has been added to the CC list.

Request Latest Update on a Case

 ✕

Problem Description *(Last updated on 07-Feb-2020, 09:18:56 PM UTC)*

Unexpected spike in DNS traffic to host 172.18.110.100 detected by Tetration Analytics Platform.

Current Status *(Last updated on 20-Feb-2020, 02:15:17 PM UTC)*

Customer is currently monitoring the implemented solution and will inform results to us.

Action Plan *(Last updated on 10-Mar-2020, 02:21:48 PM UTC)*

- (1) Customer - Monitor the system for 1 week and provide confirmation that the policy is working well or report any related issues.
- (2) Customer - Upgrade software to NX OS 6.2(10)S16 is scheduled on 3/18, monitor system stability.
- (3) Engineer - Close case after customer provides confirmation.

Resolution Summary *(Last updated on 07-Feb-2020, 09:18:56 PM UTC)*



Issue was mitigated by rerouting DNS traffic from 10.x.x.x network to a blackhole and storing 10% in the data collection server. SDN Controller policy to automatically detect issue and take rerouting action has been developed, tested and provided to customer.






Proactive Recommendation:

The syslog message "%KERN-2-SYSTEM_MSG: Invalid cksum" is observed in a number of Nexus 7K switches. The root cause of this message is due to CSCtz27004. Workaround is to reload the device. Customer needs to upgrade to NX OS 6.2(10)S16. Recommendation has been provided to customer's support team and AS engineers.

/request-update 687405514

Thanks! I have informed the case owner to review and provide you the latest case update

Enter message  

Rate your experience    Chat in WebEx Teams  Start Over  Help

Notification to Engineer



Chidambaram Arunachalam, carunach@cisco.com has requested case owner to review and provide the latest update regarding the case [683752332](#). Please reach out to customer.

Provide Case Closure Confirmation

close case 687405514

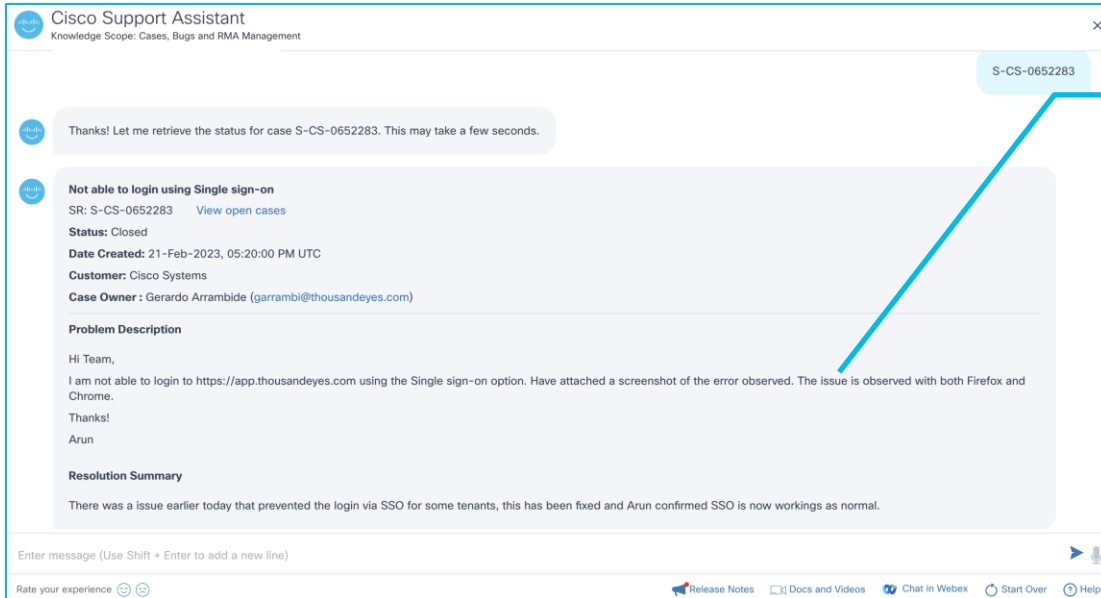
Sure. I will inform the case owner to close this case.
Thanks!

Notification to Engineer



carunach@cisco.com has requested to close the case [683752332](#).
Please take next steps. Thanks!

Get Case Status: ThousandEyes Case Summary



Cisco Support Assistant
Knowledge Scope: Cases, Bugs and RMA Management

S-CS-0652283

Thanks! Let me retrieve the status for case S-CS-0652283. This may take a few seconds.

Not able to login using Single sign-on
SR: S-CS-0652283 [View open cases](#)
Status: Closed
Date Created: 21-Feb-2023, 05:20:00 PM UTC
Customer: Cisco Systems
Case Owner : Gerardo Arrambide (garrambi@thousandeyes.com)

Problem Description
Hi Team,
I am not able to login to <https://app.thousandeyes.com> using the Single sign-on option. Have attached a screenshot of the error observed. The issue is observed with both Firefox and Chrome.
Thanks!
Arun

Resolution Summary
There was a issue earlier today that prevented the login via SSO for some tenants, this has been fixed and Arun confirmed SSO is now workings as normal.

Enter message (Use Shift + Enter to add a new line)


Rate your experience 😊 😐 😞


[Release Notes](#) [Docs and Videos](#) [Chat in Webex](#) [Start Over](#) [Help](#)

Problem Description is the initial email sent to support@thousandeyes.com by customer or the transcript of the initial chat session with ThousandEyes support engineer.

Prerequisite: External users must have their Cisco.com account and ThousandEyes account with the **same primary email address.**

Get Case Status: Duo Case Summary

 Thanks! Let me retrieve the status for case 01276088.

**Duo Push Notification isn't working**
SR or Case #: 01276088 [View case details in Duo Support Ticket Portal](#)
Status: Solved
Date Created: 09-May-2023, 11:21:33 AM UTC (Days Open: 0)
Customer: Cisco TAC
Customer Contact Name: TAC FastStart (tacfaststart@gmail.com)
Customer Contact Phone: +19197447009
Case Owner: Igor Belopolsky
Support Phone Number: <https://duo.com/support>

Prerequisite: External users must have their Cisco.com account and Duo account with the **same primary email address**.

Proactive TAC Alerts



Proactive TAC Alerts Based on My Products of Interest

The screenshot displays the Cisco Proactive TAC Alerts interface. At the top right, a light blue button labeled 'proactive TAC alerts' is visible. Below it, a section titled 'Please choose the scope of the Proactive TAC alerts.' contains two buttons: 'Case' and 'Products of my interest'. The 'Products of my interest' button is selected. The main content area, also titled 'Products of my interest', shows a list of proactive TAC alerts. The first alert is for 'Cisco 4400 Series Integrated Services Routers' and includes sections for 'Trending Issues' and 'Tool updates'. A blue arrow points from a text box on the right to the 'Products of my interest' section.

proactive TAC alerts

Please choose the scope of the Proactive TAC alerts.

Case Products of my interest

Products of my interest

Proactive TAC Alerts based on the products of interest to you
(The product list was determined based on cases opened by you within the last 12 months)

Cisco 4400 Series Integrated Services Routers

Trending Issues (Currently observed in the field)

- [FN - 72323](#)
Cisco IOS XE Software: QuoVadis Root CA 2 Decommission Might Affect Smart Licensing, Smart Call Home
- [CSCvz89043](#)
Prevent SIP services from being blocked even if license usage ACK was not received

Tool updates

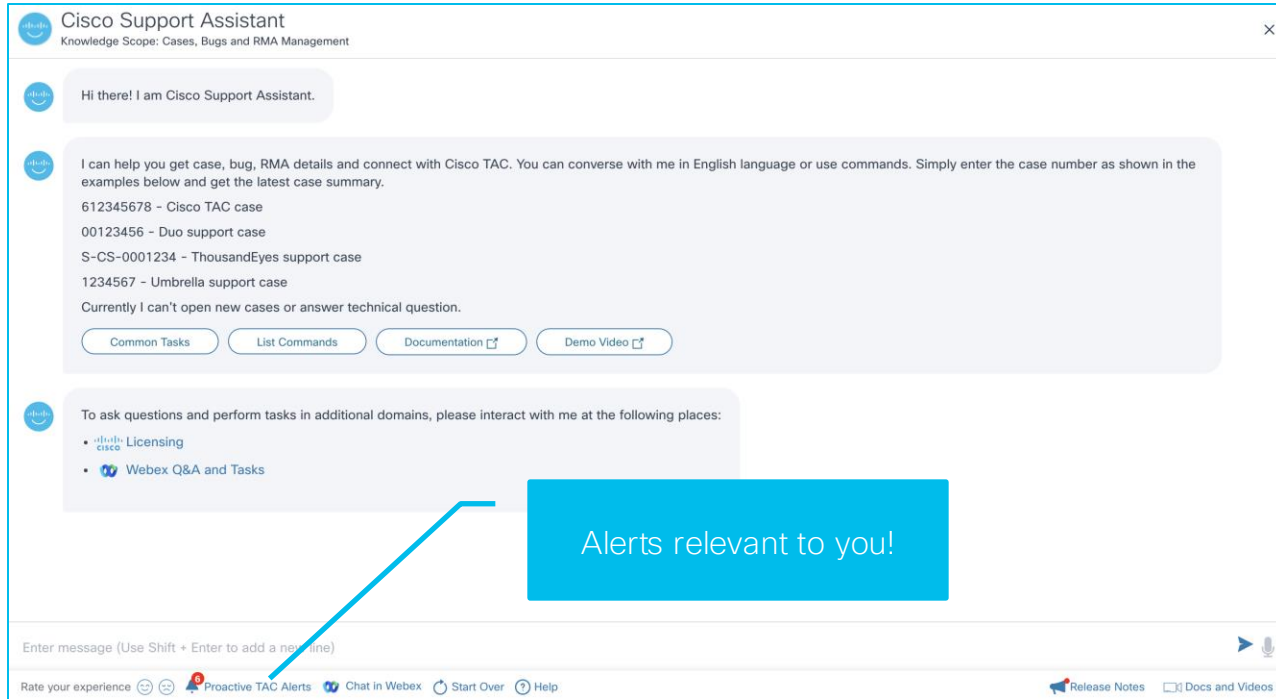
- [Log Advisor for CUBE](#)
Learn about Log collection best practices for common troubleshooting scenarios
- [Cisco Local Gateway Configuration Validator in Webex Control Hub](#)
Quickly identify configuration related issues in Cisco Local Gateways and take remediation actions.

Articles and Bulletin updates

- [Enroll Cisco IOS Managed Gateways to Webex Cloud](#)
Learn how to install Gateway connector. This is a prerequisite for Cisco Local Gateway configuration validation in Webex Control Hub.

Product list determined based on cases opened in the last 12 months

Proactive TAC Alerts Based on My Products of Interest



The screenshot displays the Cisco Support Assistant interface. At the top, it says "Cisco Support Assistant" and "Knowledge Scope: Cases, Bugs and RMA Management". The main chat area shows a greeting: "Hi there! I am Cisco Support Assistant." followed by a detailed message: "I can help you get case, bug, RMA details and connect with Cisco TAC. You can converse with me in English language or use commands. Simply enter the case number as shown in the examples below and get the latest case summary." Below this, several case numbers are listed with their corresponding product names: "612345678 - Cisco TAC case", "00123456 - Duo support case", "S-CS-0001234 - ThousandEyes support case", and "1234567 - Umbrella support case". A note states, "Currently I can't open new cases or answer technical question." Below the text are four buttons: "Common Tasks", "List Commands", "Documentation", and "Demo Video". Further down, a message says, "To ask questions and perform tasks in additional domains, please interact with me at the following places:" followed by a list: "• Cisco Licensing" and "• Webex Q&A and Tasks". A blue callout box with the text "Alerts relevant to you!" has a line pointing to the "Proactive TAC Alerts" icon in the bottom navigation bar. The bottom bar also includes "Rate your experience", "Chat In Webex", "Start Over", "Help", "Release Notes", and "Docs and Videos".

Cisco Support Assistant
Knowledge Scope: Cases, Bugs and RMA Management

Hi there! I am Cisco Support Assistant.

I can help you get case, bug, RMA details and connect with Cisco TAC. You can converse with me in English language or use commands. Simply enter the case number as shown in the examples below and get the latest case summary.

612345678 - Cisco TAC case
00123456 - Duo support case
S-CS-0001234 - ThousandEyes support case
1234567 - Umbrella support case

Currently I can't open new cases or answer technical question.

Common Tasks List Commands Documentation Demo Video

To ask questions and perform tasks in additional domains, please interact with me at the following places:


- Cisco Licensing
- Webex Q&A and Tasks

Alerts relevant to you!

Enter message (Use Shift + Enter to add a new line)


Rate your experience Proactive TAC Alerts Chat In Webex Start Over Help Release Notes Docs and Videos

Proactive TAC Alerts Based on My Products of Interest



Hi there! I am Cisco Support Assistant.

11:39:30



I can help you get case, bug, RMA details and connect with Cisco TAC. You can converse with me in English examples below and get the latest case summary.

612345678 - Cisco TAC case

00123456 - Duo support case

12345678 - Meraki support case


S-CS-0001234 - ThousandEyes support case


1234567 - Umbrella support case


Currently I can't open new cases or answer technical question.

Common Tasks



List Commands

Documentation 

Demo Video 









To ask questions and perform tasks in additional domains, please interact with me at the following places:


-  Licensing
-  Webex Q&A and Tasks

11:39:30


Enter message (Use Shift + Enter to add a new line)

Rate your experience  

 Proactive TAC Alerts  Chat in Webex  Start Over  Help

 Proactive TAC Alerts

Get Proactive TAC Alerts delivered straight to your inbox




[Manage in Notification Manager](#) 

Trending Issues

■ CSCvz89043

Prevent SIP services from being blocked even if license usage ACK was not received

Applicable for: Cisco 4400 Series Integrated Services Routers




  

■ CVE-2023-20198

TALOS Blog

Cisco IOS XE Software Web UI Privilege Escalation Vulnerability

Applicable for: Cisco 4400 Series Integrated Services Routers




  

Tool updates

■ SIP Profile Tester for CUBE and SIP TDM Gateways

Quickly validate IOS XE SIP profile configuration using sample SIP messages.




Applicable for: Cisco 4400 Series Integrated Services Routers

■ Log Advisor for CUBE

Learn about Log collection best practices for common troubleshooting scenarios




Applicable for: Cisco 4400 Series Integrated Services Routers

■ Cisco Local Gateway Configuration Validator in Webex Control Hub

Quickly identify configuration related issues in Cisco Local Gateways and take remediation actions.

Applicable for: Cisco 4400 Series Integrated Services Routers

Articles and Bulletin updates

Subscribe to automatically receive relevant alerts via email on a bi-weekly basis

© 2025 Cisco and/or its affiliates. All rights reserved.

Proactive TAC Alerts Based on My Products of Interest



Manage your notifications

Review or change the resources you receive from Cisco Customer Experience. You can also choose resources to share with your teammates.

Use your Cisco ID to get started.

[Log in to Notification Center](#)



Proactive TAC Alerts Based on My Products of Interest

The screenshot shows the Cisco Notification Manager web interface. On the left is a sidebar with navigation links: 'Welcome carunach@cisco.com', 'Notification manager' (highlighted), 'Personal settings', 'FAQ', and 'Log out'. The main content area has a dark blue header with the Cisco logo and the title 'Notification Manager'. Below the header is a sub-header explaining the purpose: 'Manage the notifications you'd like to receive, and share resources with your teammates. Your selections won't impact required communications you'll still receive from Cisco.' A light blue banner contains a tip: 'Get emails for Proactive Technical Assistance Center (TAC) Alerts by moving its toggle to "Active".' with a link 'Review and manage>'. The interface lists three notification categories: 'Renewals', 'Buying programs', and 'Services'. Each category has a toggle switch set to 'Active' and a 'Share' button. The descriptions for each category are: 'Monthly email reminders with details of expiring or expired contracts and licenses.', 'Email guidance on Cisco Enterprise Agreement (EA) license management, consumption reports, and True Forwards.', and 'Email guidance and data-driven insights for your purchased Cisco services.'

Notification Manager

Manage the notifications you'd like to receive, and share resources with your teammates. Your selections won't impact required communications you'll still receive from Cisco.

Get emails for Proactive Technical Assistance Center (TAC) Alerts by moving its toggle to "Active".
[Review and manage>](#)

Renewals [Share](#)

☒ Active | Monthly email reminders with details of expiring or expired contracts and licenses.

Buying programs [Share](#)

☒ Active | Email guidance on Cisco Enterprise Agreement (EA) license management, consumption reports, and True Forwards.

Services [Share](#)

☒ Active | Email guidance and data-driven insights for your purchased Cisco services.

Click "Review & Manage" to go right to the PTA email subscription option

Proactive TAC Alerts Based on My Products of Interest

Support

Share

Active | Proactive Technical Assistance Center (TAC) Alerts

Emails about issues and tool updates for your products of interest, based on TAC cases you've opened within the past 12 months.

Active | Support insights and recommendations

Emails with risk mitigation tips and recommended support coverage for your hardware and software. Includes Service Attach and Network and Support Insights.

Active | Last Date of Support (LDoS) insights

Emails for hardware or software purchases approaching LDoS.

Questions?

Find answers that can help you navigate and manage Notification Center.

Get answers

Proactive TAC Alerts Based on My Products of Interest

Support

Share

Share support notifications with others

Select the notifications you want to share with people on your team.

☒ Proactive Technical Assistance Center (TAC) Alerts ⓘ

☒ Support insights and recommendations ⓘ

☒ Last Date of Support (LDoS) insights ⓘ

Email

tacfaststart@gmail.com

⚙️ +

[Add another person](#)

Optional

These are useful notifications from Cisco!

By providing an alternative contact, you represent and warrant that you have the necessary rights and permissions to provide such alternative contact(s) to us. Further, you acknowledge that critical information may not be received by your organization if you provide an invalid email address.

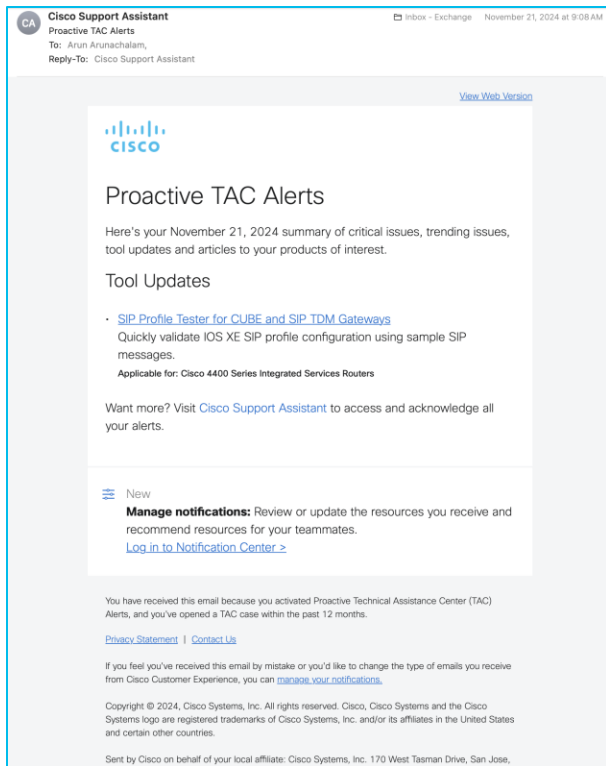
Send Invite

Close

Share your subscription with your colleagues easily!

© 2025 Cisco and/or its affiliates. All rights reserved.

Proactive TAC Alerts Delivered Right To Your Email Inbox



Conversations: Engineer Communication



Connect to Engineer - Phone Callback

connect to engineer

Would you like to use the case number 690223946? Please enter 'Yes' to use this case number or provide another case number.

Yes

Cancel

Yes

How would you like to connect with engineer?

Phone

Virtual Meeting

Cancel

Phone

Please enter a valid phone number with country code and without dashes (-). Example: 19191234567

Telephone Number

Ext (Optional)

+1

9193926009

Submit

Cancel

+19193926009

Thanks! let me check if the current case owner is available to call you. This will take about 4 minutes.

Engineer is available and will call you soon at +19193926009. Thanks!

Engineer **is** available

Connect to Engineer – Join a Virtual Meeting

connect to engineer

Would you like to use the case number 690223946? Please enter 'Yes' to use this case number or provide another case number.

Yes Cancel

Yes

How would you like to connect with engineer?

Phone Virtual Meeting Cancel

Virtual Meeting

Please provide the meeting details for the troubleshooting session:

Meeting URL

Meeting Number

Meeting Password

Submit Cancel

Thanks! let me check if the current case owner is available to join the meeting. This will take about 3 minutes.

Engineer is available and will join the meeting. Thanks!

Engineer **is** available

Connect to Engineer

Current time is **outside**
Engineer's working hours

connect to engineer



Thanks! let me check if the current case owner is available to call you.



Current time is outside the case owner's working hours (09:00 - 18:00 Monday - Friday EST).



Engineer is not available right now. Please leave a message to the engineer

Have a question about the workaround. Please callback.



Your message has been sent and the engineer will call back. If you need immediate assistance, please call Cisco TAC and request the case to be reassigned. Cisco TAC phone numbers: <https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>

Connect to Engineer

connect to engineer

Would you like to use the case number 690223946? Please enter "Yes" to use this case number or provide another case number.

Yes

How would you like to connect with engineer?

Phone

Please enter a valid phone number with country code and without dashes (-). Example: 19191234567

+19193926009

Thanks! let me check if the current case owner is available to call you. This will take about 4 minutes.

Engineer is not available right now. Please leave a message to the engineer.

Testing

Your message has been sent and the engineer will call back. If you need immediate assistance, please request the case to be reassigned using the command "requeue 690223946".

Engineer **isn't** available

Connect to Engineer

Engineer **isn't** available
right now, but will callback in
15 / 30 / 60 minutes



You 8:10 AM

connect to engineer 689629891



What is your phone number? Please enter a valid phone number including the country code without the + or - signs. Example: 491701234567



You 8:10 AM

19193926009



Thanks! Let me check if an engineer is available to call you.

Engineer is not available right now and will call back in 15 minutes.

Connect to TAC Frontline

The screenshot displays a chat interface for connecting to TAC Frontline. It features a light blue header with a "connect to engineer" button. The main chat area has a light blue background. A system message in a light blue bubble asks for a valid case number, with input fields for "Submit", "Cancel Request", and "I don't have a case number". A second system message asks if the user wants to chat with a Customer Service Representative, with "Yes" and "No" buttons. A status message indicates the user is in the queue. A third status message confirms the user is now chatting with Pushark. Two green bubbles from Pushark contain the messages: "Hello TAC FastStart and welcome to Support Case Manager assistance. You are now chatting with Pushark." and "Greetings for the day, Hope you are having a great day". At the bottom, there is a text input field with a placeholder "Enter message (Use Shift + Enter to add a new line)", a send button, and a microphone icon. The footer contains links for "Release Notes", "Docs and Videos", "Chat in Webex", and an "End Chat" button.

connect to engineer

Please enter a valid case number.

Submit Cancel Request

I don't have a case number

Would you like to chat with a Customer Service Representative?

Yes No

We're connecting you to a Customer Service Representative. You're number 1 in the queue.

You are now chatting with Pushark.

Hello TAC FastStart and welcome to Support Case Manager assistance. You are now chatting with Pushark.

Greetings for the day, Hope you are having a great day

Enter message (Use Shift + Enter to add a new line)


Release Notes Docs and Videos Chat in Webex End Chat

Select this option for
non-case related questions.
Example: Contracts


Conversations: Virtual Spaces



Use Virtual Space as the Communication Preference



 You 8:45 PM

/create-space 687202983




Communication preference has been changed from Email to Virtual Space.
You will be invited to a Webex Teams virtual space in which you can interact with the case owner and share files related to this case.

Webex Virtual Space
with case contacts and owner

 ☆ Cisco TAC Case : 687202983 : Test case 

This starts the "Cisco TAC Case : 687202983 : Test case" space, created by CiscoTAC.Spark (bot), 8:45 PM

CiscoTAC.Spark (bot) added you to this space. Welcome, 8:45 PM

 CiscoTAC.Spark (bot) 8:45 PM

Welcome [Chidambaram](#). Please use this virtual space to communicate with [Chidambaram](#), the engineer assigned to your case. The engineer will review the information provided for the following customer symptom and will contact you shortly in this virtual space.

Customer Symptom:

Technology: Cloud and Hybrid Products
Subtechnology: Collaboration Meeting Room (CMR) - Hybrid
Problem Code: Configuration Assistance

Product: N/A
Product Family: N/A
Software Version: N/A
Router/Node Name: N/A

Problem Details: Test case

Engineer contact details:

Name: [Chidambaram Arunachalam](#)
Email address: carunach@cisco.com
Phone number: +1 919 392 6009

Customer File Upload Guidelines:

<http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html>
Files shared in this space that are 300MB or less will automatically be available as case attachments. Use CSC File Uploader to share large files:
<https://cway.cisco.com/csc/index.html?requestID=687202983>

Assistant is automatically added to external virtual space

Cisco TAC Case : 696169484 : Test case ☆

Meet


Messages People (5) Content Meetings + Apps

🔍 🔍 ⚙️

Customer File Upload Guidelines:
<http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html>
Files shared in this space that are 300MB or less will automatically be available as case attachments. Use CSC File Uploader to share large files:
<https://cway.cisco.com/csc/index.html?requestID=696169484>

Conversation Transcript:
The transcript of this virtual space is available in Support Case Manager and can be downloaded as a pdf file even after the case is closed. Please click "View Transcript" button in the following link to view and download the transcript:
<https://mycase.cloudapps.cisco.com/696169484/summary>

CiscoTAC.Spark (bot) added 3 people to this space. ✓

 Support Assistant 9/16/23, 10:06 AM




Hello! I can help you get case details and connect with Cisco TAC. You can make the following requests in English language:

- @Support what is the status
- @Support change status to cisco pending
- @Support add participant (email address)
- @Support connect with engineer
- @Support create a virtual space
- @Support request an update
- @Support update the case
- @Support escalate
- @Support raise severity
- @Support requeue
- @Support close the case

I can help you manage cases that are opened from [Cisco.com Support Case Manager](#). Currently, I can't open new cases or answer technical questions. Type **`/list commands`** to get a list of command requests and find details of supported features using the [documentation](#) and [demo](#). ✓


Assistant performs tasks in the context of the TAC case associated with the external virtual space

Automatic Diagnostics Data Collection Suggestions

  Cisco TAC Case : 690611893 : Test case - Diagnostics suggestion integration 

Meet

Messages People (6) Content Schedule Add +

 CiscoTAC.Spark (bot) 1/8/21, 10:36 PM


Based on Tech: "Voice - Communications Manager Additional Apps and Plugins", SubTech: "Jabber (Mobile Devices) - Audio/Video Quality", & ProblemCode: "Error Messages, Logs, Debugs" selected while opening the case, here are steps to gather debug/techsupport logs and/or links to useful documentation.

1. Walkthrough video showing how to create a Jabber problem report ==> <https://video.cisco.com/detail/video/5979227091001/jabber---create-a-problem-report?autoStart=true&q=Jabber%20problem%20report>
2. Walkthrough video showing how to how to clear Jabber Cache ==> <https://video.cisco.com/detail/video/5835977589001/jabber---how-to-clear-cache?autoStart=true&q=clear%20Jabber%20Cache>

How to upload:

1. <https://cway.cisco.com/csc/index.html?requestID=690611893&referrer=AutoTSTeam>

Proactively collecting and uploading the technical support data allows the Cisco Technical Support team to begin investigating your Service Request more quickly and efficiently.

 CiscoTAC.Spark (bot) 1/8/21, 10:37 PM

Hi Arun , Arun Arunachalam will be working with you on this case. Please find contact details below:

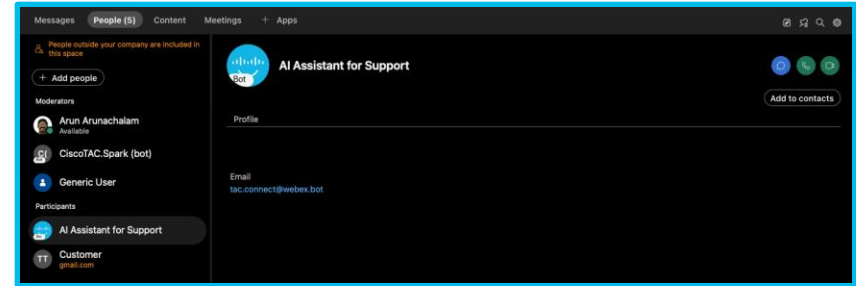
Name: Arun Arunachalam

Email address: carunach@cisco.com

Phone number: +1 919-392-6009

Virtual Space Features

- Case owners are added as moderator.
- Files up to **300MB** can be shared in the space and are transferred to case.
- When the case is closed
 - All Cisco human participants are removed
 - Automatic import of text messages
 - Virtual space is deleted after 14 days
- Conversation Transcript is available in Support Case Manager
- Customers can add authorized participants using
@(AI Assistant for Support) add-participant <email-addr>



Change Case Status to Cisco Pending

Cisco TAC Case : 691817812 : Test case Meet

Messages People (5) Content Schedule + Apps

Test case
SR: 691817812 [View case details in SCM](#)

Severity: 3 **Status:** Customer Pending
Date Created: 16-Jul-2021, 11:21:11 AM UTC (Days Open: 15)
Last Updated: 31-Jul-2021, 10:43:49 PM UTC

Customer: CISCO SYSTEMS
Case Owner: Arun Arunachalam (arunach@cisco.com)
Case Owner Phone: +19193926009
Case Owner Working Hours: Monday - Friday , 09:00 - 21:00 EDT
Case Owner Manager: Marc Holloman (mholloma@cisco.com)
Manager Phone: +1919-392-7144

Latest Information from Case Notes:

Problem Description (Last updated on 31-Jul-2021, 10:42:12 PM UTC)
Router is experiencing intermittent reload.

Current Status (Last updated on 31-Jul-2021, 10:42:12 PM UTC)
Request customer to provide crashinfo logs.

Action Plan (Last updated on 31-Jul-2021, 10:42:12 PM UTC)
Analyze crashinfo logs once received.

Customer (@gmail.com) 6:44 PM
Hi Arun, I have uploaded the logs from the device to the case. Please analyze and let me know your findings. Thanks!

TAC /cisco-pending

TAC Connect (bot) 6:45 PM
Customer, Thanks! Let me change the status to Cisco Pending.
Customer, Case status is updated to Cisco Pending.

Write a message to Cisco TAC Case : 691817812 : Test case

Customers can provide the requested information and change the case status to Cisco Pending.

Participant Authorization Checks

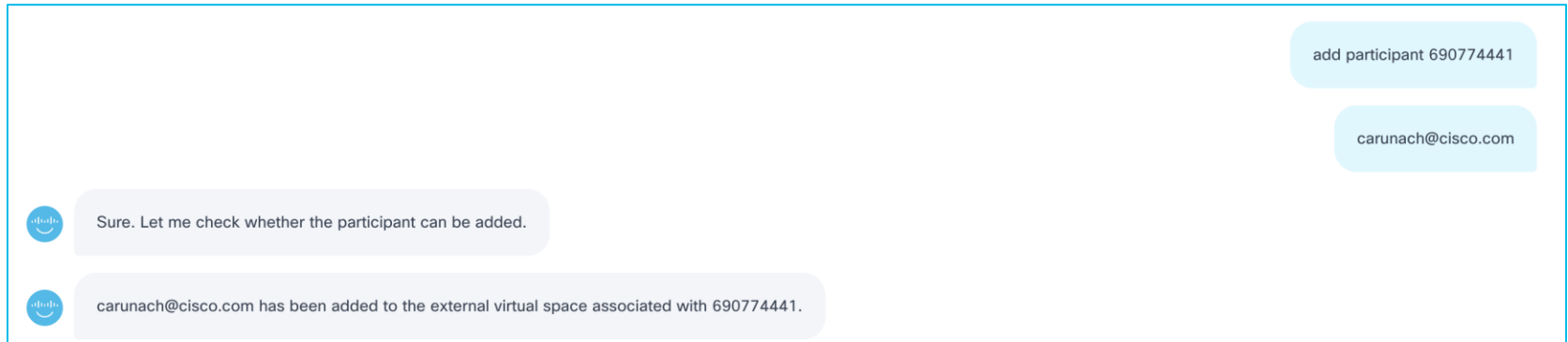
Email addresses in the CC-List of the case are automatically added to the Virtual space at the time of external space creation. Customer is informed of the list of participants who are in the CC-list but **don't have access to the case**.



CiscoTAC.Spark (bot) Sunday, 1:24 AM

Customer The participants <tac.rtpms+user2@gmail.com, ic2user1@gmail.com> that you are adding to the virtual space do not have access to this case and will be added to this space for troubleshooting purposes only. If you would like to provide access to this case please request the participants to follow Cisco's standard user registration/access request process.

Add Yourself to the Virtual Space If Authorized



The screenshot shows a chat window with a white background and a blue border. On the right side, there are two light blue input fields. The top one contains the text "add participant 690774441" and the bottom one contains "carunach@cisco.com". On the left side, there are two light blue response bubbles, each preceded by a small circular icon with a blue smiley face. The first bubble contains the text "Sure. Let me check whether the participant can be added." and the second bubble contains the text "carunach@cisco.com has been added to the external virtual space associated with 690774441."

add participant 690774441

carunach@cisco.com

Sure. Let me check whether the participant can be added.

carunach@cisco.com has been added to the external virtual space associated with 690774441.

Users can add themselves to the external virtual space if they are authorized to access the case

Participant Authorization Checks


Case owner can add participants using “Add People” button in Webex app. Case owner is informed if the participant being added **doesn't have access to the case**.




CiscoTAC.Spark (bot) Yesterday, 10:45 PM


Arun Arunachalam The participant ic2user3@gmail.com that you are adding to the virtual space does not have access to this case and will be added to this space for troubleshooting purposes only. If you would like to provide access to this case please request the participant to follow Cisco's standard user registration/access request process.


Add Authorized Participants to the Virtual Space


 You 11:03 AM
TAC add participant fegarrid@cisco.com

 TAC Connect (bot) 11:03 AM
Customer, Sure. Let me check whether the participant can be added.

CiscoTAC.Spark (bot) added Felipe Garrido to this space. 11:03 AM


 TAC Connect (bot) 11:03 AM
Customer, fegarrid@cisco.com has been added to the space.


 You 11:35 AM
TAC add participant ic2user3@gmail.com

 TAC Connect (bot) 11:36 AM
Arun, Sure. Let me check whether the participant can be added.
Arun, ic2user3@gmail.com doesn't have case access and hence can't be added to the space.


Cisco employees who already have access to the case can add another participant. The new participant is allowed **if they have case access**.

Add Authorized Participants to the Virtual Space


 Customer (@gmail.com) Yesterday, 10:54 PM
TAC add participant ic2user3@gmail.com


 TAC Connect (bot) Yesterday, 10:54 PM
Customer, Sure. Let me check whether the participant can be added.

Customer, ic2user3@gmail.com doesn't have access to this case. Hence it will require your explicit approval to add the user to this virtual space for troubleshooting purposes. Please enter 'Yes' or 'No' to approve / disapprove. Thanks!

 Customer (@gmail.com) Yesterday, 10:54 PM
TAC yes

CiscoTAC.Spark (bot) added IC2 User3 to this space. Yesterday, 10:54 PM

 CiscoTAC.Spark (bot) Yesterday, 10:54 PM
Customer The participant ic2user3@gmail.com that you are adding to the virtual space does not have access to this case and will be added to this space for troubleshooting purposes only. If you would like to provide access to this case please request the participant to follow Cisco's standard user registration/access request process.


 TAC Connect (bot) Yesterday, 10:54 PM
Customer, ic2user3@gmail.com has been added to the space.

Customers who already have access to the case can add another participant. If the new participant doesn't have case access, they will be requested for **explicit approval**.

Conversation Messages


Support Case Manager

Details for Chidambaram Arunachalam (carunach)

 >

☆ 690404206

Test case for Virtual Spaces

ASK THE BOT 


< 4 / 12 >


Summary


Notes


Attachments


Virtual Spaces

View case in CSOne 

 Launch Webex Teams

ADD NOTES 


ADD FILES 

SAVE AS PDF 

Cisco Internal

Actions	Virtual Space Title	Created Date
VIEW TRANSCRIPT	Cisco TAC Case : 690404206 : Test case for Virtual Spaces	11/30/2020 at 06:27:25

Click
"View Transcript"

Virtual Space Transcript for case 687925946 

2019-11-17 12:02:13 (GMT) carunach@cisco.com
Thanks!

2019-11-17 12:02:11 (GMT) carunach@cisco.com
This is a test case to test the View Transcript feature introduced in SCM.

2019-11-17 12:01:55 (GMT) carunach@cisco.com
Hello!

2019-11-17 12:00:52 (GMT) ciscotacspark@webex.bot
Welcome Chidambaram. Please use this virtual space to communicate with Chidambaram, the engineer assigned to your case. The engineer will review the information provided for the following customer symptom and will contact you shortly in this virtual space. Customer Symptom: Technology: Cloud and Hybrid Products Subtechnology: Collaboration Meeting Room (CMR) - Hybrid Problem Code: Configuration Assistance Product: N/A Product Family: N/A Software Version: N/A Router/Node Name: N/A Problem Details: Test case Engineer contact details: Name: Chidambaram Arunachalam Email address: carunach@cisco.com Phone number: +1 919 392 6009 Customer File Upload Guidelines: <http://www.cisco.com/c/en/us/about/security-center/tac-customer-file-uploads.html> Files shared in this space that are 300MB or less will automatically be available as case attachments. Use CSC File Uploader to share large files: <https://cway.cisco.com/csc/index.html?requestID=687925946>

Save as PDF

Cancel

Conversations: Case Handling Tasks



Raise Case Severity



You 2:28 PM

raise severity 683752332



I can increase the case severity. Please note that you are expected to be available for live troubleshooting of severely degraded network conditions impacting your business. Would you like to continue? Please respond with **yes** or **no**. Thanks!



You 2:28 PM

yes



What is your phone number? Please include the country code. Example: 491701234567.



You 2:28 PM

19193926009



Let me check the availability of the current case owner.

Engineer is not available. However, a Customer Service Representative will call you soon to increase the severity to S2 and to connect you to the next available engineer.

Requeue a Case



You 12/14/18, 1:28 PM

/requeue 684345515



I can check whether the current case owner is available to talk with you. Would you like me to check? Please type "Yes" or "No".



You 12/14/18, 1:28 PM

yes



Can the engineer call you at 19197447009? Please enter "Yes" to use this phone number or provide another phone number.



You 12/14/18, 1:28 PM


yes




Thanks! Let me check if the engineer is available to call you

Engineer is available and will call you soon at 19197447009. Thanks!

Schedule Dispatch a Case

 You 12:26 PM


requeue 689382051




Please select when you would like to requeue?

Now


Specific Time



If your case is requeued, it will change ownership to different engineer. This may increase resolution time. Would you still like to requeue?

 You 12:27 PM

yes



Please select a specific date and time. If it's the same day, choose a time slot that starts at least 1 hour ahead.

Date

2020-08-15


Time Slot

08:00 AM - 10:00 AM

Time Zone

America/New_York

Submit



1


Thanks! Let me request the requeue.

Your case is set to be requeued on 2020-08-15 during the time slot 08:00 AM - 10:00 AM hours, America/New_York. New engineer will contact you after the case is accepted.

Escalate Case

escalate 697272855

02:09:57



An escalation request will inform a manager that the case needs attention. The manager, duty manager or customer service representative will contact you to discuss further. If you would like to raise severity or requeue the case, please use the options below.


Escalate Case

Raise Severity

Request New Engineer

Cancel Request

02:09:57



Please select the escalation reason:

☐ Delay in case assignment.

☐ Delay in resolution.

☐ Delay in response.

☐ Missed commitments.

☐ High business impact.

☒ Other.

Escalation reason comments (mandatory if you select "Other" option):

Testing

Submit

Cancel Request

02:10:25

Escalate Case

02:10:23

Cisco AI Assistant for Support informs High Touch Operations Managers (HTOM) when a case is escalated by SP Advantage, TS Advantage or High Touch Expert Care customers.

Escalate Case

The screenshot displays a chat interface with a Cisco AI Assistant. The assistant's messages are in light blue bubbles on the left, and user responses are in light blue bubbles on the right. The process involves escalating a case to a TAC Manager, confirming an email address, and receiving contact information for the manager.

Assistant Messages (Left):

- 02:11:02: How would you like to proceed?
Buttons: [Escalate to TAC Manager](#), [Cancel Request](#)
- 02:11:31: Please confirm or update your email address.
Input field:
Buttons: [Submit](#), [Cancel](#)
- 02:11:59: Contacting the manager of the engineer assigned to this case.
- 02:12:05: Manager carunach@cisco.com will email you at tacfaststart@gmail.com between 01:00 and 23:30, Monday - Friday, America/Los_Angeles timezone.

User Messages (Right):

- 02:10:23: Escalate Case
- 02:11:23: Escalate to TAC Manager
- 02:11:54: tacfaststart@gmail.com

Cisco AI Assistant for Support connects you with the case owner's manager or the interim manager who will reach out to you regarding the escalation request.

Escalate Case

Escalate Case

11:04:37

How would you like to proceed?

Escalate to TAC Manager

Cancel Request

11:06:16

Please confirm or update your email address.

Submit

Cancel

11:06:54

Contacting the manager of the engineer assigned to this case.

11:07:22

Case owner's manager (carunach@cisco.com) is not available.

11:07:25

I'll contact a duty manager next. This may take up to 6 minutes.

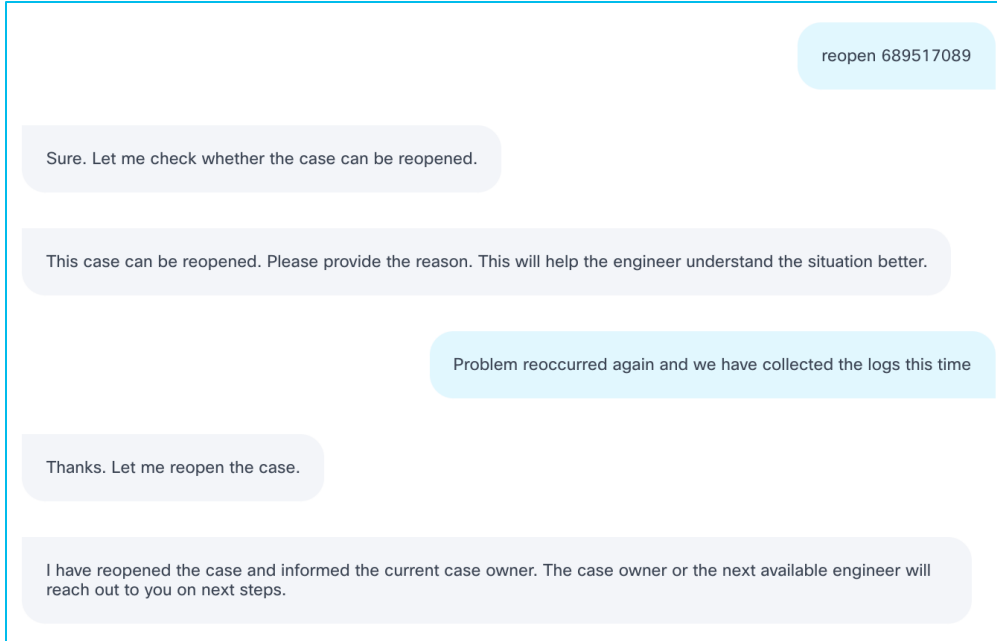
11:07:25

The duty manager will email you at tacfaststart@gmail.com.

11:08:22

Cisco AI Assistant for Support connects you with TAC Duty Manager if the case owner's manager, or the interim manager contact is not available.

Reopen a Case



The screenshot shows a chat window with a light gray background. At the top right, there is a light blue button with the text "reopen 689517089". Below this, the chat history consists of several messages in rounded rectangular bubbles. The first bubble is light blue and says "Sure. Let me check whether the case can be reopened." The second bubble is light gray and says "This case can be reopened. Please provide the reason. This will help the engineer understand the situation better." The third bubble is light blue and says "Problem reoccurred again and we have collected the logs this time". The fourth bubble is light gray and says "Thanks. Let me reopen the case." The fifth bubble is light gray and says "I have reopened the case and informed the current case owner. The case owner or the next available engineer will reach out to you on next steps."

reopen 689517089

Sure. Let me check whether the case can be reopened.

This case can be reopened. Please provide the reason. This will help the engineer understand the situation better.

Problem reoccurred again and we have collected the logs this time

Thanks. Let me reopen the case.

I have reopened the case and informed the current case owner. The case owner or the next available engineer will reach out to you on next steps.

Cases that are closed within the last 14 days
can be reopened.

Conversations: Bug Applicability Checks



Get Bug Status

CSCvn75597

Thanks! Let me retrieve the status for bug CSCvn75597. This may take a few seconds.

Cisco IOS XE Software HTTP Server Denial of Service Vulnerability
CSCvn75597

- **Status** : Fixed
- **Product** : cbr-8
- **Severity** : Severe(2)
- Click [here](#) to view known affected and fixed releases.

Bug Release-note

Symptom:

A vulnerability in the HTTP server code of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the HTTP server to crash.

The vulnerability is due to a logical error in the logging mechanism. An attacker could exploit this vulnerability by generating a high amount of long-lived connections to the HTTP service on the

Enter message (Use Shift + Enter to add a new line)

Rate your experience 😊 😞

Release Notes

Docs and Videos

Chat in Webex

Start Over

Help

Contextual Task: Check Bug Applicability

https://tools.cisco.com/security/center/softwarechecker.x

See Vulnerable Products Section of the advisory for full details:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-httperv-dos#vp

Workaround:

Please refer to the Security Advisory.

Further Problem Description:

Please refer to the Security Advisory.

PSIRT Evaluation:

The Cisco PSIRT has assigned this bug the following CVSS version 3 score. The Base CVSS score as of the time of evaluation is 5.3:

https://tools.cisco.com/security/center/cvssCalculator.x?version=3.0&vector=CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

CVE ID CVE-2019-12659 has been assigned to document this issue.

Additional information on Cisco's security vulnerability policy can be found at the following URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

Check Bug Applicability

Click the task to get started

Enter message (Use Shift + Enter to add a new line)

Rate your experience 😊 😞

Release Notes


Docs and Videos

Chat in Webex


Start Over

Help

Check Bug Applicability: Upload Diagnostic Logs





Check Bug Applicability




The output of the following commands are required to check the applicability of CSCvn75597. It is required to have the **device prompt** for each command in order to have the file processed correctly. Please enter the commands in the **full form** (no command abbreviations) as shown below in the device, collect the command outputs in a log file and upload it.

```
device# show version
device# show running-config
device# show inventory
```


 CSCvn75597-Applicable.txt • 6.64 KB  Completed

✓ Uploaded 100%



✓ Processed








Please wait while I analyze the uploaded file. This takes about 1-2 minutes.




...


Enter message (Use Shift + Enter to add a new line)  

Rate your experience 😊 😞

 Release Notes  Docs and Videos  Chat in Webex  Start Over  Help


Check Bug Applicability: View Results and Options






The output of the following commands are required to check the applicability of CSCvn75597. It is required to have the **device prompt** for each command in order to have the file processed correctly. Please enter the commands in the **full form** (no command abbreviations) as shown below in the device, collect the command outputs in a log file and upload it.

```
device# show version
device# show running-config
device# show inventory
```


 CSCvn75597-Applicable.txt • 6.64 KB Completed

✓ Uploaded 100%


✓ Processed



Please wait while I analyze the uploaded file. This takes about 1-2 minutes.





CSCvn75597 is **applicable** to your device ISR4431/K9 running on IOS-XE 16.8.1.








Here are some possible options for you.

[Software Upgrade](#) [View Advisory Summary](#) [View Fixed Releases](#) [View Additional Info](#) [Re-run Check](#)


Enter message (Use Shift + Enter to add a new line)




Rate your experience 😊 😞

 Release Notes  Docs and Videos  Chat in Webex  Start Over  Help


Check Bug Applicability: Software Upgrade Suggestion



[View Advisory Summary](#)




A vulnerability in the HTTP server code of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause the HTTP server to crash. The vulnerability is due to a logical error in the logging mechanism. An attacker could exploit this vulnerability by generating a high amount of long-lived connections to the HTTP service on the device. A successful exploit could allow the attacker to cause the HTTP server to crash. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. This advisory is available at the following link:
<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190925-httperv-dos>





Here are some possible options for you.






[Software Upgrade](#)




Please consider upgrading to IOS-XE 17.6.3a. This software is a Cisco Suggested release and has the fix for CSCvn75597. Please consult with your partner or Cisco professional services team as needed

Enter message (Use Shift + Enter to add a new line) 


Rate your experience 😊 😞

 Release Notes  Docs and Videos  Chat in Webex  Start Over  Help

Check Bug Applicability: View Fixed Releases





[View Fixed Releases](#)



 List of releases that have the bug fix based on information available in **Known Fixed Releases** field of [CSCvn75597](#):






- 16.10.2
- Gibraltar-16.11.1
- Gibraltar-16.11.1a
- Gibraltar-16.11.1b
- Gibraltar-16.11.1c
- Gibraltar-16.11.1s
- Gibraltar-16.12.1a
- Gibraltar-16.12.1b
- Gibraltar-16.12.1c
- Gibraltar-16.12.1d
- Gibraltar-16.12.1e
- Gibraltar-16.12.1s

Please visit [Software download](#) page to download the software image.

Enter message (Use Shift + Enter to add a new line)

Rate your experience  

 Release Notes  Docs and Videos  Chat in Webex  Start Over  Help

Check Bug Applicability: RADKit Based Data Collection



Hello! I can help you check the applicability of a bug to your device. You can make the following requests in English language:

[Check CSCwh87343](#)

[Status CSCwh87343](#)

[Feedback](#)

[Check CSCwh87343](#)



The output of the following commands are required to check the applicability of CSCwh87343.

device# show running-config

device# show inventory

device# show version

How would you like to provide the command outputs?

You can use Remote Automation Development Kit ([RADKit](#)) service to allow me to automatically collect the required diagnostics data in a secure fashion.

[Manually Upload Log File](#)

[Auto-collect Using RADKit](#)

[Auto-collect Using RADKit](#)



Please enable John Watson (jhwatson@cisco.com) to access the device for the next 15 minutes. After enabling access, provide details of your RADKit service. Please reference the following articles on how to enable access:

- [Adding devices](#)
- [Adding remote users](#)
- [RBAC using labels](#)

RADKit Service ID

Device name in RADKit

[Submit](#)

[Cancel](#)

Check Bug Applicability: RADKit Based Data Collection



RADKit Service ID: xxxx-xxxx-xxxx

Device Name in RADKit: cube1



Thank you! Let me check connectivity to the device. This may take a few minutes.



I'm able to connect to the device. Let me collect the commands. This may take a few minutes.



All set to go! Have collected all the required commands. Please wait while I analyze the diagnostics data. This takes about 1-2 minutes.



The device ISR4451-X/K9 running IOS-XE is **susceptible** to CSCwh87343.



Here are some possible options for you.



View Advisory
Summary



View Fixed
Releases



View Additional
Info



Send Analysis
Summary



Re-run Check

List of Supported Bugs

Hello!

Thanks for taking the time to use me. Please find below the list of bugs supported for applicability check:

BUG CATEGORIES

Supported Bugs by Software

Supported Bugs by Product

Supported Bugs by Software

IOS XE

CSCvn75597 : Cisco IOS XE Software HTTP Server Denial of Service Vulnerability
CSCvy11981 : Controller ends abnormally due to WNCD (AP name length greater and equal to 32 characters)
CSCvz30708 : Controller stops sending RADIUS packets to the RADIUS server when accounting is enabled
CSCvt89337 : Incorrect Source IP when resolving DNS
CSCvj72294 : memory leak @ CCSIP_SPI_CONTR
CSCvx71141 : Cisco Catalyst 9800-80 Wireless Controller crashes due to a CPU hog in the RRM process
CSCvw13018 : MS Teams interop CUBE: Buffer or block SIP BYE message sent by CUBE on SIP REFER scenarios
CSCvx00521 : QuoVadis root CA decommission impacting Smart Licensing and Smart Call Home Functionality
CSCwb13784 : APs not able to join 9800 due to invalid path MTU in AP Join request
CSCwc47544 : C9105/C9120/C9130 Access Points manufactured starting in September 2022 may require code upgrades
CSCvz89043 : Prevent SIP services from being blocked even if license usage ACK was not received
CSCvw74609 : LACP Configuration lost: channel-group X "mode active" gets removed on reload
CSCwd37092 : Cisco 2800,3800,4800,1562,6300 series AP:Slow TCP downloads, failing EAP-TLS in 8.10.181.0/17.3.6 SW
CSCvz59495 : Accounting Requests messages sent in a stream causes issues in the RADIUS server
CSCvw23507 : NACM rule config is missing permit all rule which causes netconf query to fail and Device in PCF
CSCvz80171 : SIP call fails egress dial-peer uses "session server-group" and "sip options-keepalive"
CSCwc68682 : 9800 controller - Link down due to local fault

AP IOS

CSCwd80290 : Cisco IOS AP image validation certificate failed/expired, causing AP join issues.

ASA

CSCvu12684 : Failover time increased after upgrading to 9.7 or later
CSCvk51778 : "show inventory" (or) "show environment" on ASA 5515/5525/5545/5555 shows up Driver/ioctl error logs
CSCvn67137 : ASA may slowly leak memory when using NetFlow

Run Bug Applicability Checks in Bug Search Tool

The screenshot shows the Cisco Bug Search Tool interface. At the top, there is a navigation bar with links for Products & Services, Support, How to Buy, Training & Events, and Partners. Below this, a breadcrumb trail shows the path: Home > CSCwd08098. The main heading is "Bug Search Tool".

The bug entry for CSCwd08098 is displayed. A modal dialog box is open, titled "Check Bug Applicability". The dialog contains the following text:

cacert.pem on FMC expired and all the devices showing as disabled.

You can now check the applicability of this bug to your device. I will request you to upload diagnostics data required to perform the check and will suggest a software version that has the fix if the bug is resolved.

☒ Don't show this message again. Got it


Below the dialog, the bug details are visible. The "Description" section includes a "Symptom" and "Logs".

Symptom:
Upgrade FMC to 6.6.5 and sensors showing as disabled after the upgrade

Logs
*Error on Device :
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Initiating IPv4 connection to 10.10.200.31:8305/tcp
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Wait to connect to 8305 (IPv4): 10.10.200.31
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Connected to 10.10.200.31 from resolved_ip_list (port 8305) (IPv4)
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] -Error with certificate at depth: 1
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] issuer = /title=InternalCA/OU=Intrusion Management System/CN=06f5f3ca-c77b-11e2-81bf-884d9d11f3ef/O=Sourcefire, Inc.
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] subject = /title=InternalCA/OU=Intrusion Management System/CN=06f5f3ca-c77b-11e2-81bf-884d9d11f3ef/O=Sourcefire, Inc.
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] err 10:certificate has expired
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] SSL_renegotiate error: 1: error:00000001:lib(0):func(0):reason(1)
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] Connect:SSL handshake failed
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [WARN] SSL Verification status: certificate has expired
*Error on FMC :
Sep 20 03:14:23 STDCD1500 SF-IMS[1504]: [4171] sftunnel:sf_ssl [INFO] VERIFY ssl_verify_callback_init

<https://bst.cisco.com/bugsearch/bug/CSCwd08098>

Run Bug Applicability Checks in Bug Search Tool

 [Products & Services](#) [Support](#) [How to Buy](#) [Training & Events](#) [Partners](#)


[Home](#) > [CSCwd08098](#)



1

Bug Search Tool

Case

I can help you check the applicability of this bug to your device. **As showing as disabled.**

CSCwd08098 |  Check Bug Applicability

 Customer Visible  Notifications [Save Bug](#) [Open Support Case](#) [View Bug in CDETS](#)

Description

Symptom:
Upgrade FMC to 6.6.5 and sensors showing as disabled after the upgrade

Logs

```
*Error on Device :
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Initiating IPv4 connection to
10.10.200.31:8305/tcp
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Wait to connect to 8305 (IPv4):
10.10.200.31
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [INFO] Connected to 10.10.200.31
from resolved_ip_list (port 8305) (IPv4)
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] -Error with certificate at
depth: 1
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] issuer =
/title=InternalCA/OU=Intrusion Management System/CN=06f5f3ca-c77b-11e2-81bf-884d9d11f3ef/O=Sourcefire,
Inc.
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] subject =
/title=InternalCA/OU=Intrusion Management System/CN=06f5f3ca-c77b-11e2-81bf-884d9d11f3ef/O=Sourcefire,
Inc.
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] err 10:certificate has expired
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] SSL_renegotiate error: 1:
error:00000001:lib(0):func(0):reason(1)
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [ERROR] Connect:SSL handshake failed
Sep 20 04:10:47 STCC2130EFW2 SF-IMS[50792]: [51982] sftunnel:sf_ssl [WARN] SSL Verification status:
certificate has expired
*Error on FMC :
Sep 20 03:14:23 STCDC1500 SF-IMS[1504]: [41711] sftunnel:sf_ssl [INFO] VERIFY ssl_verify_callback_initial
```

Run Bug Applicability Checks in Bug Search Tool

The screenshot displays the Cisco Support Assistant web interface. At the top, the Cisco logo is on the left, and navigation links for 'Products & Services', 'Support', 'How to Buy', 'Training & Events', and 'Partners' are in the center. On the right, a user profile icon and the name 'Arun Arunachalam' are visible. The main content area is titled 'Cisco Support Assistant' with a subtitle 'Knowledge Scope: Bug Applicability Checks'. A chat bubble from the assistant says: 'Hello! I can help you check the applicability of a bug to your device. You can make the following requests in English language: Check FN74214/CSCwd08098, Status CSCwd08098, Feedback'. A user input bubble contains 'Check FN74214/CSCwd08098'. The assistant's next response says: 'Please login to the Firewall Management Center (FMC) via SSH, collect the following command outputs in a log file and upload it. This will help me determine the software version and UUID of the device. Example: > show version'. Below this is a dashed box with an 'Upload a File' button and a note '(Note: File size should be less than 50MB)'. At the bottom, there is a text input field with the placeholder 'Enter message (Use Shift + Enter to add a new line)' and a blue send button. Below the input field is a 'Rate your experience' section with two smiley face icons. On the far right, there are links for 'Release Notes', 'Supported Bugs', 'Start Over', and 'Help'.

Cisco Support Assistant
Knowledge Scope: Bug Applicability Checks

Hello! I can help you check the applicability of a bug to your device. You can make the following requests in English language:
Check FN74214/CSCwd08098
Status CSCwd08098
Feedback

Check FN74214/CSCwd08098

Please login to the Firewall Management Center (FMC) via SSH, collect the following command outputs in a log file and upload it. This will help me determine the software version and UUID of the device.
Example:
> show version

Upload a File
(Note: File size should be less than 50MB)


Enter message (Use Shift + Enter to add a new line)

Rate your experience 😊 😞

Release Notes Supported Bugs Start Over Help

Run Bug Applicability Checks in Cisco Field Notice Page

<https://www.cisco.com/c/en/us/support/docs/field-notices/742/fn74214.html>



Products and ServicesSolutionsSupportLearnPartners

Trials and demos

Search

... / Cisco Firepower 4100 Series / Field Notices /

Field Notice: FN74214 – Cisco Firepower Management Center: Root Certificate Firepower Threat Defense Devices To Become Unmanaged – Software Upgrade

Products Affected

Problem Description

Problem Symptom

Workaround/Solution

Updated: November 18, 2024 Document ID: FN74214

Critical

Impact Rating: Critical

First Published: 2024-Nov-18

Last Published: 2024-Nov-18

Revision: 1.0

Cisco Bug IDs: CSCwd08098

Notice

THIS FIELD NOTICE IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTY OF MERCHANTABILITY. YOUR USE OF THE INFORMATION ON THE FIELD NOTICE OR MATERIALS LINKED FROM THE FIELD NOTICE IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO UPDATE THIS FIELD NOTICE AT ANY TIME.

Products Affected

Affected Software Product	Affected Release	Affected Release Number	Comments
Firepower Management Center Software	6	6.2.3, 6.2.3.1, 6.2.3.10, 6.2.3.11, 6.2.3.12, 6.2.3.13, 6.2.3.14, 6.2.3.15, 6.2.3.16, 6.2.3.17, 6.2.3.18, 6.2.3.2, 6.2.3.3, 6.2.3.4, 6.2.3.5, 6.2.3.6, 6.2.3.7, 6.2.3.8, 6.2.3.9, 6.4.0, 6.4.0.1, 6.4.0.10, 6.4.0.11, 6.4.0.12, 6.4.0.13, 6.4.0.14, 6.4.0.15, 6.4.0.16, 6.4.0.17, 6.4.0.18, 6.4.0.2, 6.4.0.3, 6.4.0.4, 6.4.0.5, 6.4.0.6,	

Cisco Support Assistant

Knowledge Scope: Bug Applicability Checks

Hello! I can help you check the applicability of a bug to your device. You can make the following requests in English language:

Check FN74214/CSCwd08098

Status CSCwd08098

Feedback

Check FN74214/CSCwd08098

Please login to the Firewall Management Center (FMC) via SSH, collect the following command outputs in a log file and upload it. This will help me determine the software version and UUID of the device.

Example:

> show version

Upload a File

(Note: File size should be less than 50MB)

Enter message (Use Shift + Enter to add a new line)

Rate your experience

Release Notes

Supported Bugs

Start Over

Help

© 2025 Cisco and/or its affiliates. All rights reserved.

IOS XE Software Hardening Assessment



Software Hardening Assessment – File Upload Option

The screenshot displays a chat window titled "Cisco Support Assistant" with a subtitle "Knowledge Scope: Cases, Bugs and RMA Management". The chat history includes:

- A user message: "generate hardening assessment" (06:05:44).
- A system message (06:05:45): "The output of the following commands are required to perform IOS XE software hardening assessment:
device# show tech-support
How would you like to provide the command outputs?
You can use Remote Automation Development Kit (RADKit) service to allow me to automatically collect the required diagnostics data in a secure fashion."
- A user message: "Manually Upload Log File" (06:05:47).
- A system message (06:05:48): "The output of the following commands are required to perform IOS XE software hardening assessment.
It is required to have the **device prompt** for each command in order to have the file processed correctly. Please enter the commands in the **full form** (no command abbreviations) as shown below in the device, collect the command outputs in a log file and upload it.
device# show tech-support"
- A system message (06:06:23): "Please wait while I analyze the uploaded file. This takes about 1-2 minutes."
- A system message (06:06:50): "Please download the IOS XE hardening assessment report (pdf) and reference IOS XE Software Hardening Guide." with a "Download" button.

The bottom of the chat window features a text input field with the placeholder "Enter message (Use Shift + Enter to add a new line)" and a "Send" button. Below the input field is a footer bar containing links for "Rate your experience", "Proactive TAC Alerts", "Chat in Webex", "Start Over", "Help", "Release Notes", and "Docs and Videos".

[Demo Video](#)


Software Hardening Assessment – RADKit Option

The screenshot displays the Cisco Support Assistant interface. At the top, it says "Cisco Support Assistant" and "Knowledge Scope: Bug Applicability Checks". A button labeled "generate hardening assessment" is in the top right. The chat history shows the following:

- Assistant:** The output of the following commands are required to perform IOS XE software hardening assessment:
`device# show tech-support`
How would you like to provide the command outputs?
You can use Remote Automation Development Kit (RADKit) service to allow me to automatically collect the required diagnostics data in a secure fashion.
- User:** Auto-collect Using RADKit
- Assistant:** Please enable John Watson (jhwatson@cisco.com) to access the device for the next 15 minutes. After enabling access, provide details of your RADKit service. Please reference the following articles on how to enable access:
 - Adding devices
 - Adding remote users
 - RBAC using labels
- Assistant:** RADKit Service ID: 6dsq-k7w7-5abz
Device Name in RADKit: rtpms-cube-1
- Assistant:** Thank you! Let me check connectivity to the device. This may take a few minutes.
- Assistant:** I'm able to connect to the device. Let me collect the commands. This may take a few minutes.
- Assistant:** Please wait while I analyze the collected information file. This takes about 1-2 minutes.
- Assistant:** Please download the IOS XE hardening assessment report (pdf) and reference [IOS XE Software Hardening Guide](#).
[Download](#)

At the bottom, there is a text input field "Enter message (Use Shift + Enter to add a new line)", a "Rate your experience" button, and links for "Release Notes", "Supported Bugs", "Start Over", and "Help".

Assessment: Not Entitled Scenario

 Cisco Support Assistant
Knowledge Scope: Bug Applicability Checks

Hello! I can help you check the applicability of a bug to your device. The device must be covered under an active Cisco service contract or subscription that is associated with your [Cisco.com](#) user profile. You can make the following requests in English language:

- Check <bug number>
- Status <bug number>
- Generate Hardening Assessment
- Feedback

generate hardening assessment

The output of the following commands are required to perform IOS XE software hardening assessment:

```
device# show tech-support
```

How would you like to provide the command outputs?
You can use Remote Automation Development Kit ([RADKit](#)) service to allow me to automatically collect the required diagnostics data in a secure fashion.

Manually Upload Log File

The output of the following commands are required to perform IOS XE software hardening assessment.

It is required to have the **device prompt** for each command in order to have the file processed correctly. Please enter the commands in the **full form** (no command abbreviations) as shown below in the device, collect the command outputs in a log file and upload it.

```
device# show tech-support
```

Please wait while I analyze the uploaded file. This takes about 1-2 minutes.


Sorry, you are not entitled to get TAC support for this device. Please ensure that the device is part of a service contract or subscription and associate the corresponding contract to your user profile using [Profile management tool](#) (Access Management tab).

Conversations: Contract Association




Add Contract To Your Cisco.com User Account Profile

add contract 200232664




Are you associating the contract to your user profile in order to open a TAC case right now?

No



Let me check whether this contract can be associated to your Cisco.com account




I wasn't able to associate 200232664 with your Cisco.com account with username svorma1 which may be due to one of the following reasons:

Your request has been sent to the contract's administrators for review. You will receive an email with the decision once processed. You may visit your Cisco.com profile at <https://id.cisco.com> to view the status of your request and send a message to the administrators, if needed.

If you need additional assistance, please send an email to web-help-sr@cisco.com with details. Thanks!


Add Contract To Your Cisco.com User Account Profile

add contract 12345



Are you associating the contract to your user profile in order to open a TAC case right now?

Yes



Please click the "Open New Case" button in [Support Case Manager \(SCM\)](#) to open a TAC case. SCM will check if your Cisco profile is associated with the contract for the product needing support. If not, you will be provided the option to request association. If you still need further assistance, please contact web-help-sr@cisco.com.

Dialog Handling



Dialog Response Timeout

Assistant waits for **10 minutes**
for a dialog response



You 3:05 AM

requeue 683752332



I can check whether the case owner is available to talk with you. Would you like me to check? It will only take about a minute.

NEW MESSAGES



Looks like you are busy with something else. Let's chat later.



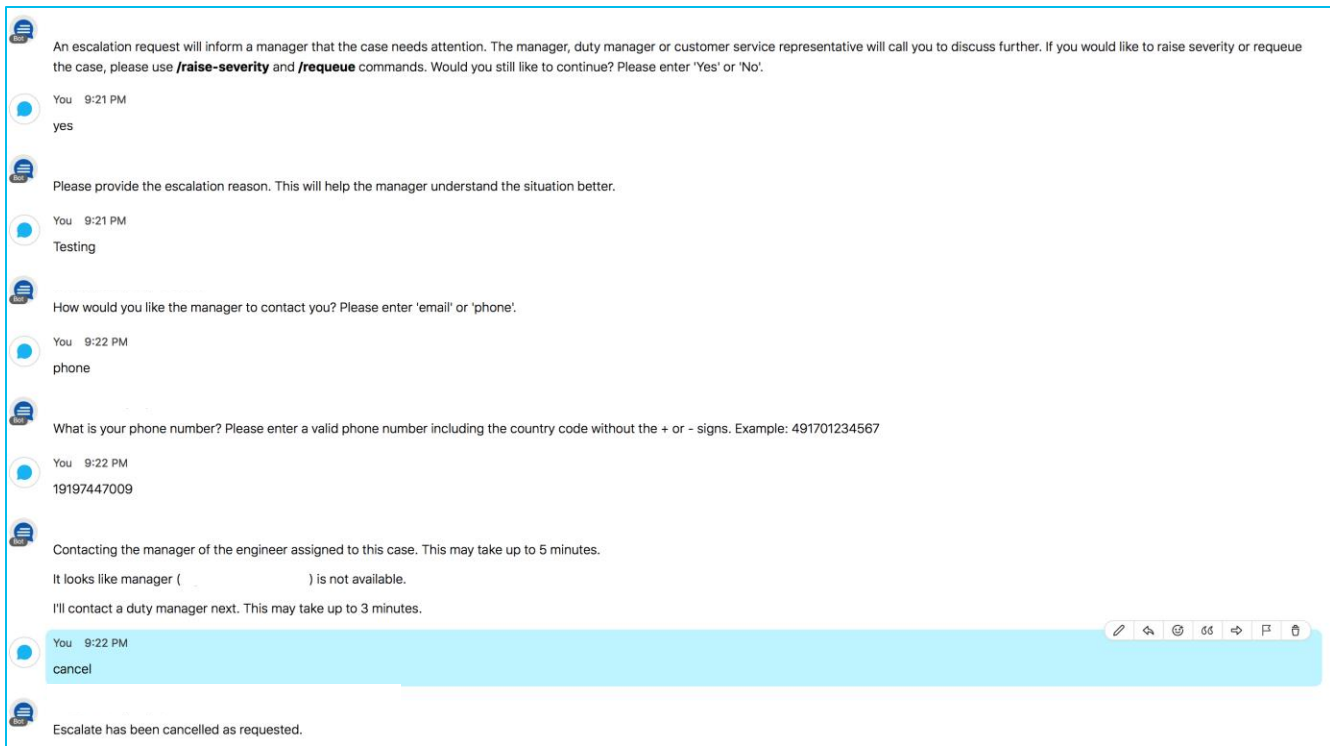
You 3:15 AM

Hello



Hello there!

Cancel In-Progress Requests



An escalation request will inform a manager that the case needs attention. The manager, duty manager or customer service representative will call you to discuss further. If you would like to raise severity or requeue the case, please use **/raise-severity** and **/requeue** commands. Would you still like to continue? Please enter 'Yes' or 'No'.

You 9:21 PM
yes

Please provide the escalation reason. This will help the manager understand the situation better.

You 9:21 PM
Testing

How would you like the manager to contact you? Please enter 'email' or 'phone'.

You 9:22 PM
phone

What is your phone number? Please enter a valid phone number including the country code without the + or - signs. Example: 491701234567

You 9:22 PM
19197447009

Contacting the manager of the engineer assigned to this case. This may take up to 5 minutes.
It looks like manager () is not available.
I'll contact a duty manager next. This may take up to 3 minutes.

You 9:22 PM
cancel

Escalate has been cancelled as requested.

Connect to Duo




Connect to Duo Support

connect to duo

Please enter your 10-digit Account ID in the format 1234-5678-90.

Submit

Please enter a valid phone number without dashes (-)

 +1 ▾

Select country code from dropdown then enter telephone number

Submit

+19193926009

Thanks! You will receive a callback from Duo Support.

Assistant calls Duo support number, informs customer's account ID to engineer and then connects to customer via callback.

Help, Commands Q&A, Feedback



Help

help

Hello! I can help you get case, bug and RMA details and connect with Cisco TAC. You can make the following requests in English language:

- [my cases](#)
- [what is the case status \(case number\)](#)
- [what is the bug status \(bug number\)](#)
- [what is the rma status \(rma number\)](#)

You can ask me to perform the following tasks:

- [connect with engineer \(case number\)](#)
- [create a virtual space \(case number\)](#)
- [request an update \(case number\)](#)
- [update the case \(case number\)](#)
- [add participant \(email address\)](#)
- [raise severity \(case number\)](#)
- [requeue \(case number\)](#)
- [escalate \(case number\)](#)
- [close the case \(case number\)](#)
- [reopen the case \(case number\)](#)
- [add contract \(contract number\)](#)

You can mark a case as favorite and get automatic notifications when the case summary (Problem Description, Current Status and Action Plan) gets updated:

- [favorite \(case number\)](#)
- [list favorites](#)
- [status favorites](#)

You can ask me to connect to support teams:

- [connect to duo](#)

You can ask me to check whether a bug is applicable to your device ([supported bugs](#)):

- [check bug applicability \(bug number\)](#)

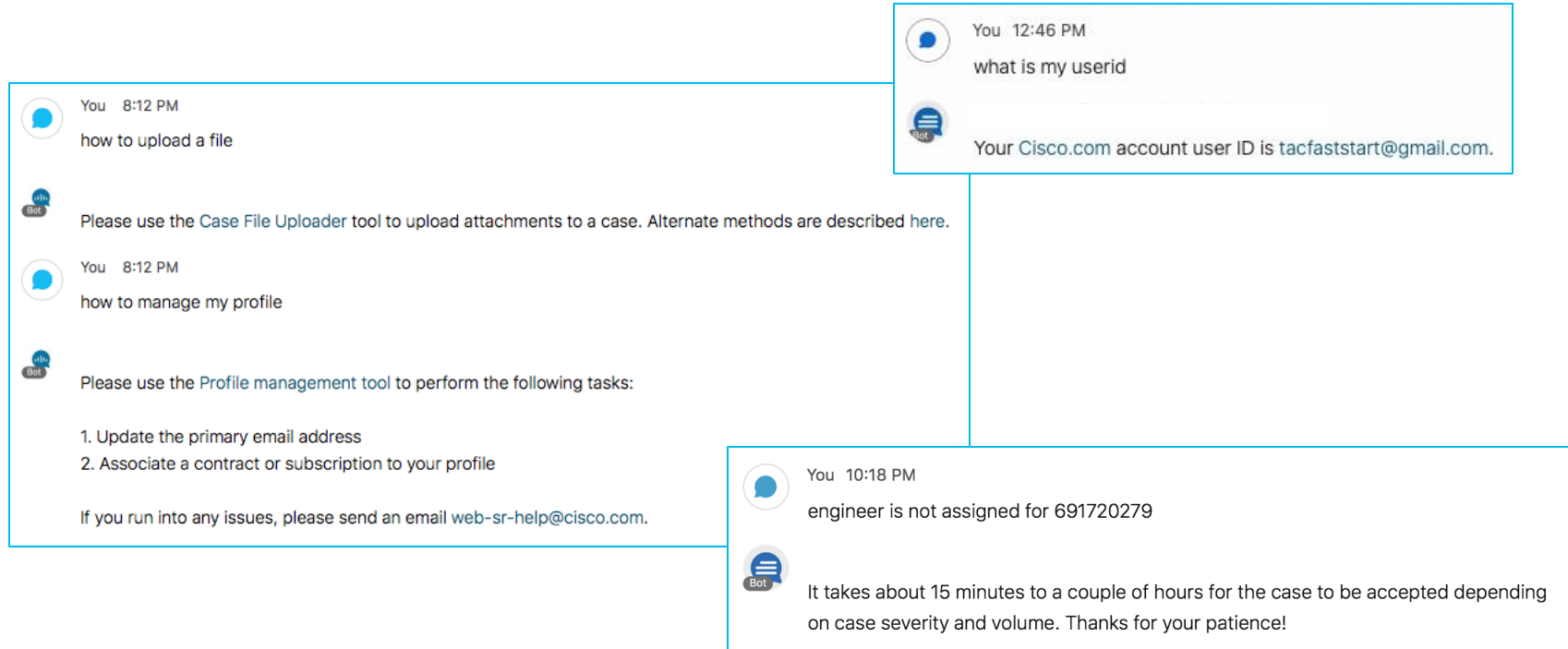
I can help you manage cases that are opened from [Cisco.com Support Case Manager](#). Currently, I can't open new cases or answer technical questions. Type **"list commands"** to get a list of command requests and find details of supported features using the [documentation](#) and [demo videos](#).

Command List

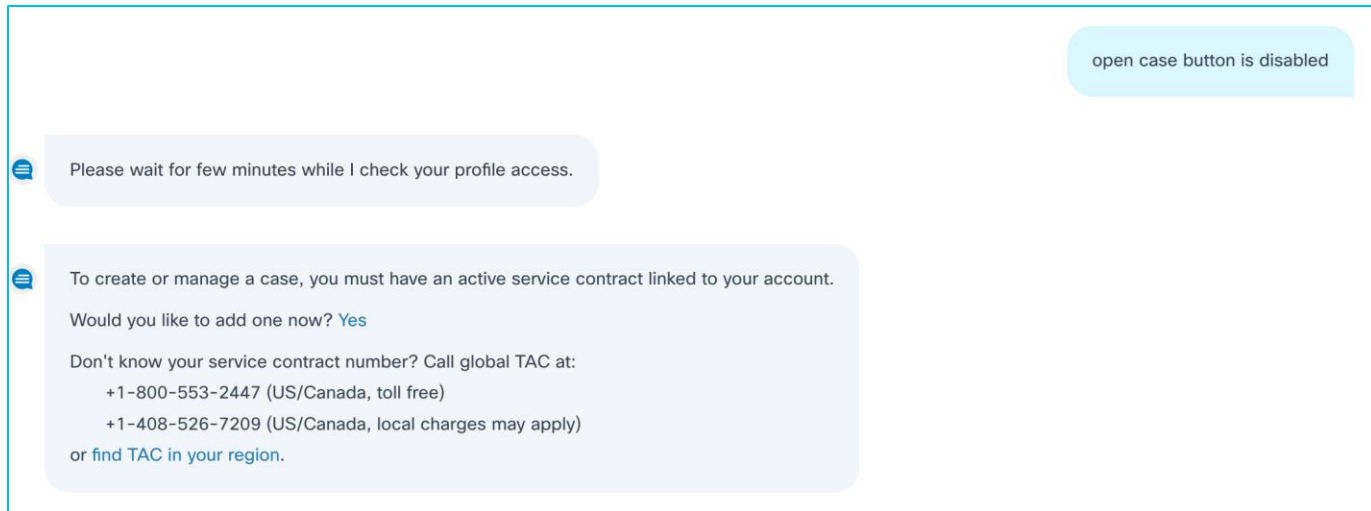
/list commands

- **/action-plan:** Sends the last note containing action plan
- **/add-contract:** Associate an active service contract to your Cisco.com user profile
- **/add-participant:** Add a participant email address to the cc-list
- **/bug:** Get list of Bugs associated with TAC case
- **/case-feedback:** Give multi-line feedback about the case in a single message
- **/check-bug-applicability:** Check applicability of a bug to your device
- **/clear** or **/reset:** Reset the conversation dialog
- **/close-case:** Request engineer to close case
- **/connect:** Connect to case owner of a case
- **/connect duo:** Connect to Duo support
- **/create-space:** Create an external Webex virtual space for a case
- **/customer:** Get customer information associated with TAC Case
- **/description:** Get problem description for the TAC case
- **/escalate:** Escalate a case
- **/favorite:** Add a case to favorite list
- **/feedback:** Give multi-line feedback about the bot or a TAC case
- **/last-note:** Get the last note from the TAC case
- **/link:** Get link to the case in Support Case Manager
- **/list cases:** View the prioritized list of your cases
- **/list favorites:** List the favorite cases
- **/owner:** Get case owner (TAC CSE) for TAC case
- **/proactive-alerts:** Get critical issues, trending issues, tool updates, latest articles and bulletins in the context of a case
- **/raise-severity:** Raise the severity of a case
- **/reopen:** Re-open a case
- **/request-update:** Request engineer to provide the latest case update
- **/requeue:** Requeue a case
- **/return-status:** Get status of parts returned in the context of a RMA
- **/rma:** Get list of RMAs associated with TAC case
- **/status:** Get status of a case, bug or RMA
- **/status favorites:** Status of favorite cases
- **/update:** Add a note to the TAC case
- **/updated:** Get the date on which the TAC case was last updated, and calculate the time since last update

Simple Case Management Related Q&A



Case Open Access Validation



The screenshot shows a chat window with a light blue header bar. In the top right corner of the header, a light blue pill-shaped button contains the text "open case button is disabled". The chat area has a white background. On the left side, there are two blue speech bubble icons. The first message is a light blue bubble from the assistant that says "Please wait for few minutes while I check your profile access." The second message is a larger light blue bubble from the assistant. It starts with "To create or manage a case, you must have an active service contract linked to your account." followed by "Would you like to add one now? [Yes](#)". Then it says "Don't know your service contract number? Call global TAC at:" followed by two phone numbers: "+1-800-553-2447 (US/Canada, toll free)" and "+1-408-526-7209 (US/Canada, local charges may apply)". It ends with "or [find TAC in your region](#)."

open case button is disabled

Please wait for few minutes while I check your profile access.

To create or manage a case, you must have an active service contract linked to your account.

Would you like to add one now? [Yes](#)


Don't know your service contract number? Call global TAC at:

- +1-800-553-2447 (US/Canada, toll free)
- +1-408-526-7209 (US/Canada, local charges may apply)


or [find TAC in your region](#).

When a user says that they can't open a case, the assistant automatically validates user's Cisco.com profile and suggests steps to get access.

Share Feedback


 You 10:49 PM

/feedback demo worked great!


 Bot

Thanks! Your feedback has been provided to my creators.

Assistant Feedback

 You 7:34 AM

/case-feedback The case was handled well

 Bot

Thanks! I have updated the case with your feedback.

Case Feedback

Notifications



Latest Release-Notes in Web Interface

The screenshot shows the Cisco Support Assistant web interface. The top navigation bar includes links for Products & Services, Support, How to Buy, Training & Events, and Partners. The user's name, Arun Aruna, is displayed in the top right corner. The main chat window is titled "Cisco Support Assistant" with a subtitle "Knowledge Scope: Cases, Bugs and RMA Management". The assistant's messages are as follows:

Hi there! I am Cisco Support Assistant.

I can help you get case, bug, RMA details and connect with Cisco TAC. You can manage cases that are opened from Cisco.com Support Case Manager. Currently I can't open new cases or answer technical question.

To ask questions and perform tasks in additional domains, please interact with me at the following places:

- [Cisco Licensing](#)
- [Webex Q&A and Tasks](#)

At the bottom of the chat window, there is a "Rate your experience" section with two smiley face icons. Below this, there is a "Release Notes" button with a red dot, which is highlighted by a blue box and a blue arrow pointing to a callout box. Other buttons at the bottom include "Docs and Videos", "Chat in Webex", "Start Over", and "Help".

Red dot (if present)
indicates new features
and bug fixes!

Latest Release-Notes in Web Interface

Hello!

Thanks for taking the time to use me. Please find the latest Release-notes below.

July 31, 2020

Enhancements:

- You can request a case to be re-opened if it was closed within the last 14 days.
- You can request a case to be schedule dispatched by specifying the date, time and time zone.
- Link to Release-notes is available in web interface.

Bug Fixes:

- Case title is missing in "my cases" response. This is applicable only for Webex Teams desktop clients.
- Concurrent requests of the same type (e.g. connect to engineer) must not be allowed.

June 28, 2020

Enhancements:

- Interact with me in the [external virtual space](#) associated with the TAC case.

June 26, 2020

Enhancements:

- You can request to be contacted via email for escalation follow-up.

Bug Fixes:

- %20 is displayed in Engineer and Manager phone number instead of space character.

May 29, 2020

Enhancements:

- Phone number input made easy in web interface!
- Case owner manager information is shown in case status response.
- The definition of case escalation is explained and confirmation obtained prior to escalation.

Automatic Release Notifications in Webex App

Notifications are sent during **your local day time**



You Yesterday, 5:24 PM

Hello!

I just got upgraded today. Please find Release-note details below:

Enhancements:

1. My creators have renamed me to [Cisco Support Assistant](#). A short demo video is available [here](#).
2. You can provide a custom reason when requesting a case to be closed.
3. Device specific Proactive TAC Alerts (critical issues applicable to your device) displayed in the context of a case are now extended to Cisco VCS Control, Cisco VCS Expressway and Cisco Jabber products.

Thanks for taking the time to use Cisco Support Assistant (formerly known as TAC Connect Bot)!

Unsubscribe Release Notifications

unsubscribe release-notes



Please let me know the reason to opt-out from Release-note notifications.

I view the Release-notes page

Submit

Cancel Request



Thanks for letting me know! You will not receive Release-note notifications in the future.



Please visit [Cisco.com page](#) and contact support-assistant@cisco.com for questions and feedback.