|  |  |  |  |
| --- | --- | --- | --- |
| Cisco Corporate Logo | Document Number | EDCS-861921 | |
| Owner | Patricia Rivera | |
| Content SME | TAC Duty Manager | |
| Last Revision Date | August 8, 2017 | |
| Next Review Date | September 1, 2018 | |
| TAC Case Escalation Process | | |

Table of Contents

[1 Purpose 3](#_Toc487012246)

[2 Scope 3](#_Toc487012247)

[3 Customer Data Protection 3](#_Toc487012248)

[4 Overview 3](#_Toc487012249)

[5 Process 4](#_Toc487012250)

[5.1 Validate Troubleshooting 4](#_Toc487012251)

[5.2 S1 and S2 System Alerts 4](#_Toc487012252)

[5.2.1 S1 and S2 System Alert Escalation Timers 4](#_Toc487012253)

[5.3 Collaborate to Obtain Assistance 6](#_Toc487012254)

[5.3.1 Case Transfer 6](#_Toc487012255)

[6 Escalating SWSS Cases 7](#_Toc487012256)

[7 Development Engineering (DE) and Customer Assurance Program Escalation 7](#_Toc487012257)

[7.1 Regional Risk Register (RRR) 7](#_Toc487012258)

[8 BU Escalation 8](#_Toc487012259)

[9 Process Compliance 8](#_Toc487012260)

[9.1 Compliance Effective Date 8](#_Toc487012261)

[9.2 Compliance Measurement 9](#_Toc487012262)

[9.3 Compliance Exceptions 9](#_Toc487012263)

[9.4 Non-Compliance 9](#_Toc487012264)

[10 Related Policy, Process, or Procedure 9](#_Toc487012265)

[11 Definitions 9](#_Toc487012266)

[12 Approvals 9](#_Toc487012267)

[13 Revision History 10](#_Toc487012268)

[Appendix A Escalation Process Flow 11](#_Toc487012269)

# Purpose

This document provides TAC Customer Support Engineers (CSEs) the process steps to execute when seeking higher levels of technical support and resources to resolve customer cases.

# Scope

This process applies to the following organizations, except those in locations where local processes exist to meet Business Unit, partner or customer requirements:

|  |  |
| --- | --- |
| **Organizations Affected** |  |
| TAC (Global/Regional) | **X** |
| High Touch Technical Support (HTTS) |  |
| Global TAC Sourced Support - Contact Center Services (TAC Front Line/TFL) | **X** |
| Global TAC Sourced Support - CSE Services |  |
| Cloud & Managed Services (CMS) |  |
| Global Service Logistics & Operations (GSLO) |  |
| Services Entitlement Team |  |
| Technical Services Product Management (TSPM) |  |
| Failure Analysis Operations (FA) |  |
| Media Convergence Server (MCS) Support |  |

# Customer Data Protection

This process may involve usage of customer-related information. CSEs should understand the importance of protecting different types of customer data. For more information about your responsibilities in customer data protection (CDP), refer to [Customer Data Protection Policies site](http://wwwin.cisco.com/c/cec/organizations/cisco-services/resources/data-protection/cdp-policy.html).

# Overview

Requests for higher levels of technical support, or Escalations, may come from customers, partners or from internal Cisco sources such as: Account Managers, Sales Engineers, etc., or may be initiated automatically through Case monitoring systems. CSEs may initiate the escalation process as well. System-generated alerts for escalations come in the form of Opera Alerts /CSOne alerts.

# Process

## Validate Troubleshooting

Engineers will work to understand and resolve customer cases by collecting information and documenting it in the Case Notes.

Research technical resources for problem solutions and document a Problem Description and Problem Statement (for KT: one object/one deviation when appropriate).

* + - Use Kepner-Tregoe (KT) methodology when appropriate (refer to [KT methodology](http://www-tac.cisco.com/kt/)).

If the issue can be duplicated, record instructions for duplicating the problem in the Case Notes.

## S1 and S2 System Alerts

System Alerts (OPERA, C3, or CSOne alerts) are system generated e-mails that provide visibility to active Cases exceeding a predetermined amount of time. The owner of the Case is expected to respond to the alert immediately. Provide the following information in written email responses:

* Provide an overview of the situation.
* List the current actions taken to resolve the issue and the status of the actions taken.
* List action plan/next steps to be taken:
  + Describe if any workarounds have been suggested to the customer, were they acceptable, if or when the workarounds will be implemented
  + Describe the severity of the technical issue
  + Describe the consequences of new occurrences, or any customer deadline expectations
  + Describe, if possible, a root cause for the customer’s problem
  + Assess what additional involvement is needed from the team or from other teams

### S1 and S2 System Alert Escalation Timers

The following table identifies automated escalation timers when an Opera Alert/CSOne Alert will be generated and requires a response.

| Elapsed Time | Severity 1 (Network Down) | Severity 2 (Severe Impact) |
| --- | --- | --- |
| 1 hour | TAC Team Alert (Mgr. copied) |  |
| 2 hour | TAC Manager (Global Mgrs. and Duty Managers copied) |  |
| 4 hours | TAC Director | TAC Team Alert (Mgr. copied) |
| 5 hours |  | TAC Manager (Global Mgrs. and Duty Managers copied) |
| 12 hours | TAC Director Second Alert |  |
| 24 hours | VP, Global Technical Center | TAC Director |
| 48 hours | President | VP, Global Technical Center |
| 96 hours |  | President |

**Monday – Friday:**

Respond to All System Alerts. If the CSE who owns the Case is unavailable for any reason, the escalation chain is as follows:

0) CSE (start with #1 if CSE unavailable)

1) Team

2) Team Manager

3) Duty Manager

4) Director

**Saturday, Sunday, and All Cisco Paid Holidays:**

Respond to All S1 and S2 System Alerts at Director level or higher using the following escalation path:

0) CSE (start with #1 if CSE unavailable)

1) Technology Team

2) Duty Manager

**Case: Status EQUALS -  Requeue, New, CE Pending, Customer Updated, DE Pending, CE Pending - Lab Recreate, CE Pending - No Contact, 3rd Party Pending**  
   
If the Case Status is anything else other than what is listed above, the timer will be stopped and no further Opera Alert/CSOne Alert will be sent out.

## Collaborate to Obtain Assistance

* + Ensure Case Title and Notes are clear and updated to reflect the actual problem
  + Make sure all the relevant e-mails/files are attached to the Case and there is mention of the relevant Cases/Bugs involved. Please refer to the [TAC Case Management Process](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/8035a269-4870-49e9-8028-19adddec1538) document for additional details.
  + Check with your colleagues (e-mail and/or face-to-face), as they may be able to assist with issue resolution.
  + If no immediate assistance available, follow the [GTAC Collaboration Process](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/888b1efc-62a1-4701-ae89-0c5c49d074ff) and tech zone to obtain assistance.
  + As a last option, send an e-mail to the relevant technical aliases (emea-xxx-esc, cs-..). For guidelines on information to include in these emails see section 5 of the [TAC Online Communities Engagement Policy](https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-970886&ver=approved).
  + For Severity 1 or Severity 2 (S1 or S2) Cases: If there is no resolution, or if the person who responds recommends that DE be involved, refer to the Development Engineering (DE) and Customer Assurance Program Escalation Section.
  + TAC: Talk to your manager, Team Lead or your technology Technical Leader (<http://www-tac.cisco.com/escalation/index.shtml>) when appropriate for operational escalation when all collaboration options are exhausted.
* If you are still unable to make progress, despite applying the above, contact the Duty Manager.
* DM Schedule for escalation:

**TAC** - <http://schedule.cisco.com/cgi-bin/schedule-parser.pl?DUTY_MANAGER>

### Case Transfer

For transferring cases, refer to the Change of Ownership section of [[GTAC Collaboration Process](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/888b1efc-62a1-4701-ae89-0c5c49d074ff)](http://wwwin-eng.cisco.com/BMS/CA/CSE_Global/1019795_TAC_Collaboration_Process.docx) . If change of ownership fails, follow [TAC Case Transfer Process](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/2a31ee8a-7388-48f1-aefd-df31a75050eb) as appropriate.

During Warm-Handoffs where TFL is involved, refer to [TFL-to-TAC Severity 1-2 Call Handoff Procedure](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/45750335-de60-4d3c-a8bf-86f7f8984d33).

Note:

Update the case with an appropriate Problem Description and Action Plan and Business Impact. Make sure the case subject/title reflects the appropriate description of the customer's problem.

# Escalating SWSS Cases

If an assigned DSM determines that the defined SLOs were not met AND the issue is impacting the customer or the customer escalates the issue to the DSM, follow the below process.

* + 1. DSM sends an email to the TAC case owner and the TAC manager of the owner of the case. During non-business hours or if the manager is not available, the available escalation program lead (CSE) will be contacted to handle this responsibility. They will include the information from [DSM Escalation Request template](https://cisco.jiveon.com/docs/DOC-1690801) into the email to explain the escalation.
    2. Within two business hours of the escalation request, the Tier 1/Tier 2 manager will review the case and provide an action plan to the DSM. The action plan will include the information in the [Escalation Action Plan template](https://cisco.jiveon.com/docs/DOC-1690802) and the action plan will be sent in an email in the TAC case.
    3. The manager will stay engaged until the action plan has been delivered/completed. If necessary and requested by the DSM, the manager will participate in update meetings with the DSM and customer.

# Development Engineering (DE) and Customer Assurance Program Escalation

Escalation processes to BU DEs are not standardized due to differences in contact method, geography, ticketing systems – event, GAMES, BEMS, etc. Engineers will become familiar with the BUs with whom they work and their specific engagement processes. For engagement information, please view: https://cisco.jiveon.com/groups/cisco-escalation

* Prior to any BU escalation, refer [BU Escalation](#_BU_Escalation) section in this document.
* CAP escalations are an exception process to be used when the normal business process has failed and there is severe ongoing customer business impact. CAP is the highest level of escalation within Cisco.
* CAP requests are generally submitted by the Cisco account team on behalf of the customer and where Cisco revenues are in jeopardy. Do not submit a CAP request without the Cisco account team and TAC manager approval.

CAP Escalation information can be found at the Cisco Escalation Tree, located at <https://cisco.jiveon.com/groups/cap-customer-assurance-program/blog/2015/09/10/cap-request-submission-guidelines>.

## Regional Risk Register (RRR)

The RRR Collaboration Tool connects Sales, Cisco Services and BUs to more effectively address escalating customer issues and maintain our customers' trust in Cisco. A new RRR is not required if a decision has already been made to engage CAP. The RRR tool is intended for use by all customer-facing managers, including Systems Engineering Managers, Service and Support managers and Service Delivery Executives. For more information on RRR escalations, visit the [Regional Risk Register page.](https://cisco.jiveon.com/groups/regional-risk-register/pages/overview)

# BU Escalation

Any questions to a BU can be emailed to the appropriate TAC technology group email alias, posted to Tech Zone or entered as a ticket to the available BU escalation ticket tool. DEs monitor TAC technology group e-mail aliases and may be able to provide support. The CSE only use the TAC technology group e-mail aliases for serious problems that the group, team leads or Technical Leaders are unable to address.

Users of legacy tools, such as C3 Forms or Webmon, use “BU Escalation” Note Type to reflect engagement of a BU. This Note Type reflects a formal escalation to the BU. This note type will also assist both Engineering and TAC management measure and monitor Cases with BU escalations.

Please review [**Appendix A**](#AppendixA) for the Escalation Flow for BEMS. Escalation link: http://bems.cisco.com/

Note:

Above note type is reserved for instances where collaborative efforts have commenced with a BU resource for a Case escalation. An e-mail to the DE/BU alias does not constitute a BU Escalation unless the e-mail alias is the escalation process for the given BU.

Work Instructions for escalating a Case to any Business Unit (BU) via Legacy tools:

1. Select ‘Internal’ for the Case note – viewable by internal Cisco only

2. Select the note type – ‘BU Escalation’

3. Within the note type, note which BU the escalation is with

4. Include the BU ticket number and URL to the ticket, when applicable

In CSOne, the note visibility is hard-coded to be Internal.

# Process Compliance

## Compliance Effective Date

This process becomes effective upon the last date of approval as noted in Cisco’s current Electronic Document Control System.

## Compliance Measurement

Compliance with Cisco processes is required. Compliance to this process may be verified through various methods, including but not limited to, reports from available business tools, internal and external audits, self-assessment, and/or feedback to the policy owner. Compliance with this policy will be enforced by TAC managers.

## Compliance Exceptions

Exceptions to the terms of this process are handled on a case-by-case basis only. Exceptions require written approval by Executive (Director or above) to non-comply for strategic business reasons. Documented exceptions and justifications will be communicated to affected technical services organizations immediately upon approval.

Any records of exceptions including Theater-specific handling requirements (local processes) should be approved and archived according to the [Cisco Records Management Process](http://wwwin.cisco.com/process/bes/iso/doc_control.shtml), and not on an individual’s laptop.

## Non-Compliance

Compliance with Cisco processes is required. Deviations or non-compliance with this process, including attempts to circumvent the stated process by bypassing or knowingly manipulating the process, system, or data may result in disciplinary actions per Cisco’s company policies, up to and including termination.

# Related Policy, Process, or Procedure

553819 [TAC Product Hazard Alert Procedure](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/e18a1b87-f139-43e8-9b8c-3192b40d2c72)

623653 [Product Security Incident Assistance Process](http://wwwin-eng.cisco.com/CA/PSIRT/Procedures/PSIAP.html)

633639 [WW CIN-to- TAC S1/S2 Phone Line Hand-Off Procedure](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/45750335-de60-4d3c-a8bf-86f7f8984d33)

1002858 [TAC Case Management Process](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/8035a269-4870-49e9-8028-19adddec1538)

731005 [TAC Case Transfer Policy and Process](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/2a31ee8a-7388-48f1-aefd-df31a75050eb)

1272658 [Mobile Internet Technology Group Escalation](https://cisco.jiveon.com/groups/mitg-escalation)

# Definitions

Defined terms are located in EDCS as [1147899 TAC Glossary of Terms](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/d38a23d0-f85e-4a6c-add6-6aab86a6f814).

# Approvals

For a record of the approval history, go to this document’s [information page](https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/04ba5a32-4053-4d73-aa39-454b42158d21).

| Organization | Name |
| --- | --- |
| TAC Americas Delivery (East) | Ullie Versavel |
| TAC Americas Delivery (West) | Hector Acevedo |
| Global TAC Sourced Support – Contact Center Services (TFL) | Brian Fady (Proxy - Brendon Nilson) |
| Global TAC Sourced Support – CSE Services | Brian Fady (Proxy - Michele Paino) |
| TAC AP Delivery | Allyn Medway |
| TAC - EMEAR | Adrian Purcarea |
| Cloud Support, CALO & Incident Mgnt | Marty Martinez |
| TS APJ+GC | Colin Soh |
| TS EMEAR | Rik Boven |
| TS Americas & HTTS | Marty Pantoja |

# Revision History

The revision history is located at the following link: https://docs.cisco.com/share/page/site/nextgen-edcs/document-details?nodeRef=workspace://SpacesStore/04ba5a32-4053-4d73-aa39-454b42158d21

#### Escalation Process Flow

