Cisco Unified Intelligence Center Release 12.0(1) ES18 COP

December 2021

[Contents](#)

Introduction

The Cisco Options Package (COP) file provides a way to deploy software outside of the normal maintenance release processes.

This document describes how to download and apply the COP file: **ciscocuic.12.0.1.18.cop.sgn**

Pre-requisites for Installing the COP

You can apply this COP file only to systems that have Cisco Unified Intelligence Center (CUIC) Release 12.0(1) FCS build 12.0.10000-48 installed or on top of earlier COP files applicable for this release.

COP	Unified Intelligence Center Standalone	Unified Intelligence Center and Live Data Co-resident	Live Data Standalone
12.0.1.18 COP	Required	Required	Required

Patch Version

File Name	MD5 sum
ciscocuic.12.0.1.18.cop.sgn	9514f4f0a64f9fdea0737d75bc7ddd76
ciscocuic.12.ES.Rollback.cop.sgn	85609a83809773cd889d1e7a4c928c1f

COP Contents and Supported Feature List

This COP includes headline fixes as listed in the **Resolved Caveats** section.

Unsupported Features

None

Known Caveats

- CSCvg44257 - CUIC 11.X columnindex out-of-sequence values in cuicreportdefinitionfield cause export failure

  Note: The 12.0 ES03 and later ES releases do not cover the import flow fix. Hence in 12.0 ES03 and later ES releases, if you import a report having non-consecutive column index, the indexes and formulae will not be corrected.

- CSCvq63127 - CUIC Differential sync fails

  Note: Even after applying 12.0 ES03 and later ES releases, the differential sync will still fail if the synced user who was deleted in CUIC is not manually restored. This fix only prevents such instances in future.

- CSCvq85385- OAMP session will be logged out if either CUIC or any other platform pages such as Cisco Unified Operating System Administration, Disaster Recovery System, and Cisco Unified Serviceability are logged in the same browser.

Special Instructions

Steps to enable external links in dashboard

Due to the security fixes added from 12.0 ES 18, dashboard widgets with external links will not work and will display blank.

To make them work run the CLI command on all nodes: `set cuic properties allow-external-links on`

Note: Ensure to restart the CUIC Reporting service after running the command on each node.

Ergonomics—Accessibility Compliance

This COP includes following accessibility enhancements:

Enhancement Detail	Action
Character Height	All font sizes used across screens meet the accessibility requirement.
Icon	All icons appearing across screens meet the accessibility requirement.
Color Contrast	All color contrast ratio across screens meets the accessibility requirement.
Color information	All color information for icons meets the accessibility requirement.
Color Conventions	All color conventions across icons and screens meet the accessibility requirement.
Visible Focus	The contrast color of a UI element is changed when that UI element gets the focus (either through mouse clicks or keyboard).

Clear Browser Cache

After Installing the Cisco Unified Intelligence Center 12.0(1) ES18 COP file, ensure that you clear your browser's cache.

User Synch from Unified CCE or Packaged CCE

You cannot perform the following actions for users who have been synched into Unified Intelligence Center from Unified CCE or Packaged CCE:

- Edit the Report Designer and the Dashboard Designer roles.
- Delete those users.
- Deactivate those users.

Download and Import Unified CCE Stock Templates

Fix for CSCvt97925: Import the latest Unified CCE stock templates when you are upgrading from CUIC 12.0(1) ES08 to the latest ES.

Configure SMTP server with TLS 1.2 secure connection

If you want the communication between Cisco Unified Intelligence Center and the mail server to be encrypted with TLS, follow the steps below to upload a Self-Signed Certificate (applicable only when the

mail server is offering a Self-Signed Certificate; these steps are not required when the mail server offers a CA-signed certificate):

1. Log in to *cmplatform* and navigate to **Security > Certificate Management**.
2. Click **Upload Certificate/Certificate Chain**. The **Upload Certificate/Certificate Chain** dialog box opens.
3. To upload the certificate chain, select **tomcat-trust** from the **Certificate Purpose** list.
4. Select the file to upload. Click the **Choose File** button and navigate to the file; then, click **Open**.
5. Click **Upload**.

2020a DST Updates

Customers who require Time Zone update 2020a should first install the CUIC 12.0(1) ES10 (or later) ES and then install the DST ES **ucos.dst-updater.tzdata-2020a-1.el7.cop**.

Configure Cross Origin Resource Sharing (When) for Live Data

In Live Data (Standalone) 12.0 deployment, when CUIC and Cisco Finesse components are in version 12.5 or later, Live Data gadgets will not load in Cisco Finesse. You must enable CORS and set Finesse host URLs to load the Live Data gadgets

Live Data CORS commands allow you to configure CORS and hence allow web applications running on different origins to communicate with Live Data and CUIC.

For Unified Intelligence Centre gadgets (Live Data) to load in Cisco Finesse, ensure that you perform the following:

- On the CUIC server,
  - Enable CORS using the `utils cuic cors enable` command.
  - Set the Finesse host URL in the `utils cuic cors allowed_origin add URLs` command.

  Note: Ensure that you restart the CUIC Reporting service after running these commands.

- On the Live Data server,
  - Enable CORS using the `utils live-data cors enable` command.
  - Set the Finesse host URL in the `utils live-data cors allowed_originadd URLs` command.

  Note: Ensure that you restart the Live Data NGNIX service after running these commands.
  Examples:
  - https://<finesse-FQDN>
  - https://<finesse-FQDN>:port

  Note:
- Ensure that you run all the preceding four CLI commands on both the nodes of CUIC and Live Data cluster.
- In the Packaged CCE and Unified CCE 2K models, CUIC and Live Data are co-resident in a system. Hence, ensure that you run all the preceding four CLI commands on this single system.

For more information on CUIC CORS CLIs, see *Administration Console User Guide for Cisco Unified Intelligence Center* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-intelligence-center/products-maintenance-guides-list.html.

For more information on Live Data CORS CLIs, see *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html.

Cisco Unified Intelligence Center Licenses

In this ES release, the application of Cisco Unified Intelligence Center licenses during fresh install or upgrade is removed.

When you install or upgrade to version 12.0(1) ES10, Cisco Unified Intelligence Center is provisioned with premium licenses. The installed premium license cannot be removed.

Administration Console User Experience Changes

This release provides an improved user experience to configure, edit, and manage the following Operation Administration Maintenance and Provisioning (OAMP) entities:

- User Management
- Device Configuration
- Log and Trace Settings
- Control Center Management
- Cluster Configuration
- Tools Management

For more information on the new user experience pages, refer OAMP 12.0 ES10 Online Help.

Upgrade from 12.0(1) ES (11) to 12.5(1)

Fix for CSCvv24801: If you are a customer, on ciscocuic.12.0.1.11.cop.sgn COP with CUIC 12.0.10000-48, you must first upgrade to the latest ES release. Upgrading to CUIC 12.5.1.10000-59 must be attempted only after installing the latest 12.0(1) ES file.

Downloading the COP File

Download the COP file **ciscocuic.12.0.1.18.cop.sgn** from the Software Download Areas – Unified Intelligence Center 12.0(1). Place the COP file on an SFTP server that can be accessed from your Cisco Unified Intelligence Center 12.0(1) servers.

Installing the COP

The following procedure describes how to use the CUIC Command Line Interface (CLI) to install the COP file.

> **IMPORTANT:** You must use the CLI to perform this upgrade. Do not use the Cisco Unified Operating System Administration page to perform this upgrade as the installation may hang.

Step 1: Log in to the Cisco Unified Intelligence Center CLI. To log in to the CLI, specify the System

Administrator username and password.

Step 2: Enter the command **utils system upgrade initiate** to start the COP installation.

Step 3: Select source **1) Remote Filesystem via SFTP**.

Step 4: Enter the remote path to the directory on the SFTP server where you downloaded the COP file.
Note:

- If the COP file is located on a Linux or UNIX server, enter a forward slash (/) at the beginning of the directory path.

  For example, if the COP file is in the patches directory, enter */patches*.

- If the COP file is located on a Windows server, check with your system administrator for the correct directory path.

Step 5: Enter the SFTP server name or IP address.

Step 6: Enter the Username and Password to the SFTP server.

Step 7: Press **Enter** to skip the prompt "Please enter SMTP Host Server (optional)".

Step 8: Wait until the system displays a list of COP files available at the SFTP location. Select the number corresponding to the COP file that you want to install.

Step 9: Type **Yes** to continue the installation.

Step 10: Reboot the machine using the command **utils system restart** after the COP installation is complete.

Step 11: Check for the deployment type:

- If this deployment is a single-node cluster, your installation ends here.

- If this deployment is multi-node cluster repeat the installation procedure (from Step 1) on other nodes.

Note: Installing the **ciscocuic.12.0.1.18.cop.sgn** COP file uninstalls the existing language pack. Hence, you must reinstall the language pack COP.

Resolved Caveats in this COP File

This COP file resolves the following caveats.

Table 1:   LiveData Caveats – Resolved in CUIC 12.0(1) ES18

Identifier	Headline
CSCwa46810	log4j2 zero day vulnerability in LiveData

Table 2:   LiveData Caveats – Resolved in CUIC 12.0(1) ES17

Identifier	Headline
CSCvz06351	Handle SocketIO Authentication token in HTTP Header

CSCvz08934	Add custom header to LiveData to be backward compatible with CUIC 12.6 ES01

Table 3:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES16

Identifier	Headline
CSCvw74324	Cisco Unified Intelligence Center Improper Error Handling
CSCvw74333	Cisco Unified Intelligence Center Misconfigured Content Security Policy
CSCvw74343	Cisco Unified Intelligence Center Misconfigured HTTP Strict Transport Security (HSTS)
CSCvw74359	Cisco Unified Intelligence Center HTTP HEAD Method enabled
CSCvw74371	Cisco Unified Intelligence Center Enabled Auto Complete in sensitive field
CSCvy35385	Address the UI issues caused by accessibility fixes
CSCvy35410	Accessibility UI issues on loading login/logout
CSCvx32124	CUIC Group configuration, stored procedure sp_get_grp_ancestors() times out.
CSCvy73552	In 12.0 ES 16, error and warning icons not appearing

Table 4:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES15

Identifier	Headline
CSCvw17076	Finesse Historical Reporting Gadget Doesn't refresh automatically
CSCvv47954	CUIC delay with accessing User Group page
CSCvu65827	When Schedule report name is changed, schedule date is set to End date
CSCvx68651	When DataSource is connected to secondary node, observed Status Icon shown in Light Green/Red Color
CSCvx68615	In Dashboard permalink, filter info (i) icon is missing for Report Widgets

Table 5:   Live Data Caveats - Resolved in CUIC 12.0(1) ES15

Identifier	Headline
CSCvx71261	When CUIC & Finesse are in version 12.6 and LD on version 12.0/12.5 observed Gadgets are not loading

Table 6:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES14

Identifier	Headline
CSCvw90969	Unable to update Collections because the number of columns in INSERT does not match the number of VALUES.
CSCvw38765	Unable to enable CORS on Live Data server.

Table 7:   Live Data Caveats - Resolved in CUIC 12.0(1) ES13

Identifier	Headline

Identifier	Headline
CSCvv65921	Unable to Set Live Data CUIC Datasource in UCCE 4k deployment.
CSCvt13475	Vulnerability (CVEsd-2015-0225) reported on ActiveMQ's JMX port(12002).

Table 8:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES13

Identifier	Headline
CSCvp37987	For UCCX Supervisors, all the CSQ values of Valuelist are displayed in the filter UI of CUIC.
CSCvv98101	Provide support for scheduled reports to be emailed using SMTP server with TLS 1.2 secure connection.
CSCvv85520	All war.backup files under platform tomcat webapp are getting exploded during tomcat restart.
CSCvv61043	CUIC 12.0 - Some Live Data Gadgets freeze on a dashboard.
CSCvv48370	The Chat Agent Detail Report shows the rating chat for only 5 values on the Selected Rating Filter.

Table 9:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES12

Identifier	Headline
CSCvu02274	CUIC 12.5 scheduler only supports SHA1 SFTP server.
CSCvv24801	Switch Version failed from CUIC 12.0(1)-ES11 to 12.5(1). **Note**: If you are a customer, on **ciscocuic.12.0.1.11.cop.sgn** COP with CUIC 12.0.10000-48, you must first upgrade to **ciscocuic.12.0.1.12.cop.sgn** COP or any later ES releases. Upgrading to CUIC 12.5.1.10000-59 must be attempted only after having the latest COP file of the previous release.

Table 10:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES11

Identifier	Headline
CSCvt99379	CUIC with UCCE doesn't allow to delete the User from CUIC.
CSCvt00310	SFTP reports is not according to the 'locale' field in the Scheduled table, and is nondeterministic.
CSCvu63088	Accessibility Enhancements for CUIC 12.0(1).

Table 11:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES10

Identifier	Headline
CSCvu40571	DST/TZ update with 2020a.
CSCvu08920	Make Call button is not visible in Agent call history tab in Finesse 12.0 with 11.6 stock reports.

Table 12:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES09

Identifier	Headline

Identifier	Headline
CSCvt97925	ES08 removes 'dataclause' while importing 'SQL query' based Reports causing Report execution failure. **Note:** Fix for CSCvt97925 needs the latest Unified CCE stock templates to be imported from CCO after installing CUIC 12.0 ES09.
CSCvp27499	Folder created inside Stock folder cannot be deleted.

Table 13:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES08

Identifier	Headline
CSCvj99730	Apache Struts ClassLoader Remote Code Execution Vulnerability.
CSCvs95030	CUIC 12.0 Groups > "AllUsers" Value List not sorted alphabetically.
CSCvt25535	CUIC Report Definition failing to save when adding new fields.

Table 14:   Identity Server Caveats - Resolved in CUIC 12.0(1) ES07

Identifier	Headline
CSCvq18547	OutofMemoryError in IdS when the SAML response is processed.
CSCvs01904	Error message showing SHA-1 Secure Hash Algorithm is not relevant for version 12.0 onwards.
CSCvq76882	CUIC: Optimization Needed on Permissions Check Process.
CSCvr72266	CUIC 'All Users' group permission for the teams synched from PCCE.
CSCvr77122	Qualys Security vulnerabilities QualysID:38739 QualysID:38738 on CUIC.
CSCvs04715	Qualys Security vulnerabilities QualysID:38739, QualysID:38738, QualysID:11827 and QualysID:13162.
CSCvs17553	Result discrepancy in CUIC Excel export when Report contains custom footer formula and NULL values.
CSCvs17818	CUIC Gauge cuts off if used in a dashboard permalink.
CSCvs38362	Unauthenticated report permalink of another node is not working in the dashboard web view widget.
CSCvs56459	Failed to import 12.5 Live Data Reports.

Table 15:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES07

Identifier	Headline
CSCvq76882	CUIC: Optimization Needed on Permissions Check Process.
CSCvr72266	CUIC 'All Users' group permission for the teams synched from PCCE.
CSCvr77122	Qualys Security vulnerabilities QualysID:38739 QualysID:38738 on CUIC.
CSCvs04715	Qualys Security vulnerabilities QualysID:38739, QualysID:38738, QualysID:11827 and QualysID:13162.
CSCvs17553	Result discrepancy in CUIC Excel export when Report contains custom footer formula and NULL values.
CSCvs17818	CUIC Gauge cuts off if used in a dashboard permalink.
CSCvs38362	Unauthenticated report permalink of another node is not working in the dashboard web view widget.

CSCvs56459	Failed to import 12.5 Live Data Reports.

Table 16:   Live Data Caveats - Resolved in CUIC 12.0(1) ES06

Identifier	Headline
CSCvs56914	Live Data reports do not load in finesse with CUIC and FINESSE in 12.5 and LD and CCE in 11.6.
CSCvs56917	Live Data Agent report import fails in CUIC 12.5 with LD and CCE in 11.6.

Table 17:   Unified Intelligence Center Caveats – Resolved in CUIC 12.0(1) ES05

Identifier	Headline
CSCvq17387	UCCE Supervisor LDAP Login with Alternate UPN doesn't map to user imported from ICM for Hybrid SSO.
CSCvr25044	After CUIC 11.6(1) ES14 upgrade, All LDAP Logins Fail if User Search base has lower case "dc".
CSCvr46346	Report definition save failure upon customization by adding new fields.
CSCvr55969	CUIC LDAP integration fails in 11.6 with COP 14 \ 15 when no 'dc' reference in User search Space.

Table 18:   Live Data Caveat - Resolved in CUIC 12.0(1) ES05

Identifier	Headline
CSCvr31094	24K deployment Live Data connection times out and datasource does not come up.

Table 19:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES04

Identifier	Headline
CSCvr16839	Incorrect Threshold Color for CUIC Gauge Report using Numeric Chart View.
CSCvr68150	CUIC reports show 1 hr TZ offset for Brasilia TZ after applying ucos.dst-updater.2019b COP.

Table 20:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES03

Identifier	Headline
CSCvg44257	CUIC 11.X columnindex out-of-sequence values in cuicreportdefinitionfield cause export failure.
CSCvo41606	UCCE Stock reports templates contain Report definitions not supported by CUIC.
CSCvo42978	Custom format for Integer fields not working.
CSCvo95897	Scheduled report emails are missing as schedules get stuck in running state.
CSCvp83951	Avoid persisting "clause" for non-filterable fields.
CSCvq63127	CUIC Differential sync fails.

Table 21:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES02

Identifier	Headline
CSCvi38366	CUIC Takes Minutes to Bring Up All Certificates in OS Admin Page.

CSCvk30995	When exporting CCX Reports, date format is incorrect.
CSCvn75618	CUIC Reports exported in Excel shows date instead of percentage.
CSCvp21140	Unable to add/remove a collection value which associated with MediaSense value list.
CSCvp71691	LD report shows "Request to server returned Unauthorized" when loaded on Finesse desktop.

Table 22:   Identity Server Caveat - Resolved in CUIC 12.0(1) ES02

Identifier	Headline
CSCvp30273	Network Scanner "Insecure Implementation of Cookie Attribute".

Table 23:   Unified Intelligence Center Caveats - Resolved in CUIC 12.0(1) ES01

Identifier	Headline
CSCvn65118	Found newly created folder is auto moved to child folder.
CSCvo01643	Not able to set default filter for MediaSense Report.
CSCvo11551	Permalinks as Finesse gadgets are not loading.
CSCvo27540	IE11: Dashboard permalink with multiple LD reporting widgets does not work with multiple refreshes.

Identifier	Headline
CSCvo47197	LD variable permalinks are not working.
CSCvo70924	CUIC inserts 'top' clause to sub SQL query which limits the output.
CSCvo98208	RFI Vulnerability in CUIC.

Rollback COP

Use the following Rollback COP file to roll back to the First Customer Shipment (FCS) version.

Note: The CUIC Rollback COP file removes all previous ESs installed on the system and reverts your system to the FCS version (in this case, Cisco Unified Intelligence Center Release 12.0 (1)).

Rollback COP file: ciscocuic.12.ES.Rollback.cop.sgn

MD5 Checksum: 85609a83809773cd889d1e7a4c928c1f

Note: To install the Rollback COP, follow the steps outlined in the Installing the COP section.