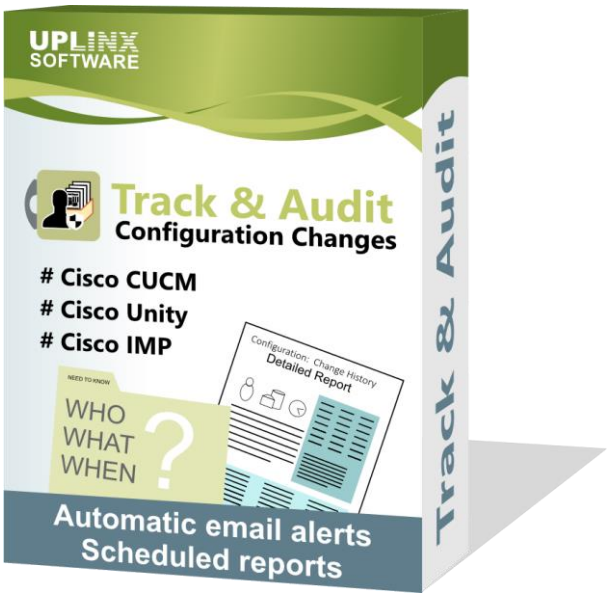
UPLINX SOFTWARE

Track & Audit
for Cisco Unified Communications

AUDITING AND ACCOUNTABILITY

March 2nd, 2020



UPLINX SLU
Camí dels Plans 53
AD400 La Massana
ANDORRA

www.uplinx.com

Audit and Accountability

Audit and accountability measures are the processes required to keep control of a complex multi-user environment. By maintaining a trace of all configuration activity on Cisco Unified Communications servers, conserving data and tracking changes as they occur, and ultimately ensuring individuals can be held accountable for their actions, UPLINX Track & Audit is the right tool for your audit, accountability and compliance requirements by capturing and storing a complete audit trail. User-restricted access to changes is easy and immediate for investigations and compliance reviews.

Audit Data Collection

Generate audit records containing information that establishes what configuration event has occurred, when and where it occurred, the previous and updated values, and the identity of the user account associated with the change.

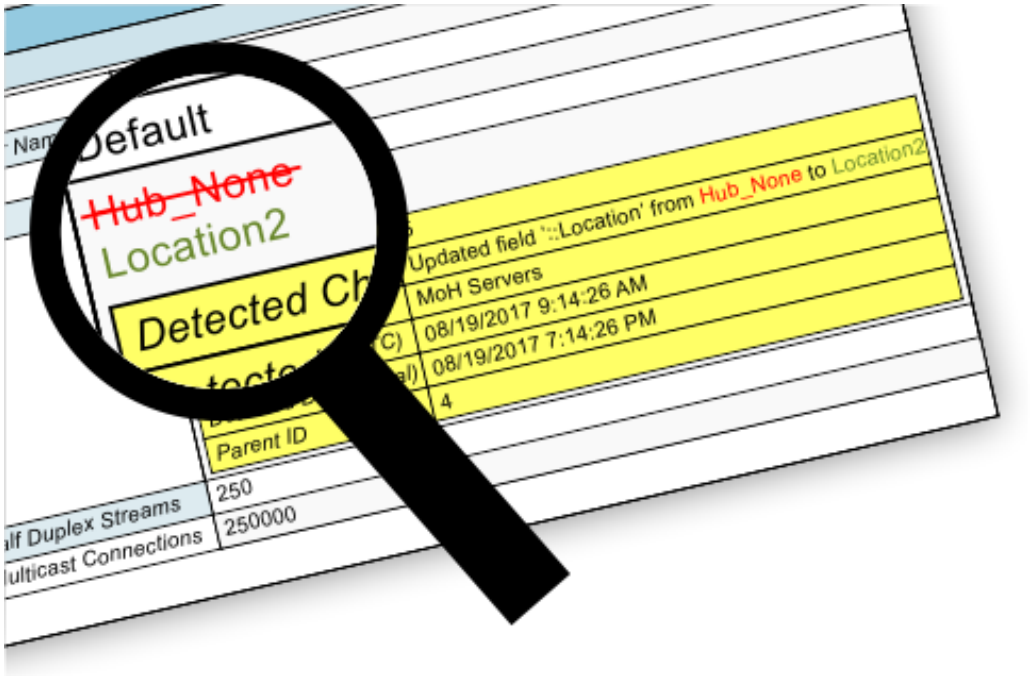
You need to …	Track & Audit Features
Collect detailed records (including Who, What and When) of configuration settings for your Cisco Unified Communications network servers.	Track & Audit provides detailed scheduled reporting on your Cisco Unified Communications Network.

Target reports by customizing report range to ensure the audit trail contains detailed information for your requirements.	Setup up individual reporting for each server, selecting which objects are to be tracked. Define multiple reports to cover different auditing requirements.
Keep track of all Cisco servers.	Track & Audit will supply audit reports on CUCM, CUC, CUPS (IM & P), CER, UCCX, UCS, Expressway, CMS, and even InformaCast and VMWare servers. See all supported Cisco servers.

Audit Record Retention

Retain audit records for the time period required by your record retention policy or by compliance regulations.

You need to …	Track & Audit Features
Store your audit data in a way that ensures easy access for incident investigations.	The Track & Audit Report Repository of configuration and comparison reports, immediately available through the Web Console, stores all reports for instant access.
Maintain a control over storage resources, allowing you to choose necessary retention policies.	Periodic Clean-up settings schedule deletion of outdated generated reports, application logs and collected Cisco Audit logs.



Perform Audit Trail Reviews

Regularly review audit records for an overview of configuration access, endpoint and user MACDs and unusual activity, to then act on findings through further investigation, personnel training or tuning asset requirements.

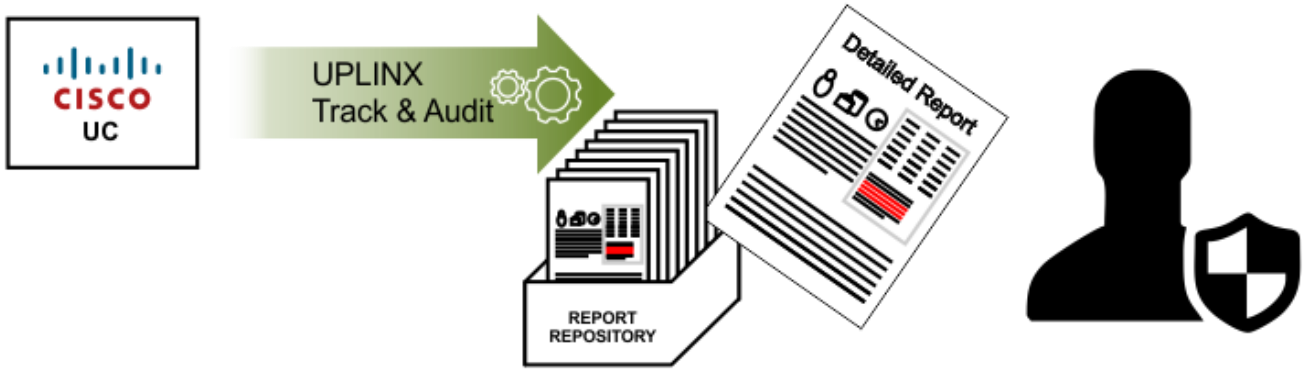
You need to …	Track & Audit Features
Regularly review a consolidated audit trail across your Cisco Unified Communications servers.	Instantly accessible Report Repository. Change Summary email notifications. Readable searchable reports in HTML format.
Configure notifications about changes on tracked objects.	Define Notification Actions to email you when a specified tracked object has changed.
Real-time alerts on critical object changes.	Track & Audit can receive and process Cisco-generated Syslog alerts to report in real time via email or trigger a comparison report for a full picture of before and after the event.
Get extra depth of reporting by utilizing the power of Cisco Audit Log information.	Track & Audit will optionally receive Cisco Audit logs for the added precision of timestamps and user info.

Read more about the Audit Console.

Report Generation and Audit Reduction

Provide summary reports to support on-demand audit review, analysis and reporting requirements and incident investigations without altering the original audit logs.

You need to …	Track & Audit Features
Receive a summary of changes without having to digest a full report until required.	Track & Audit can send a summary of changes after comparison report generation
Customize scope of reports to focus on items of interest depending on your requirements	Track & Audit allows precise selection of which objects to track per report, from the full list of hundreds of different objects available.
For any diff report, choose if it needs to be a complete status report or just show the changes	Choose to generate full comparison reports with changed and unchanged items, or to only report on tracked changes.



View sample reports online.

Response to Audit Processing Failures

Monitor for audit processing failures and take corrective actions to restore normal audit capturing process.

You need to …	Track & Audit Features
Monitor the status of audit data collection.	Track & Audit keeps track of itself with its own Status Monitor service. Scheduling and Report functionality is constantly monitored.
Alert Administrators about audit failures.	If the core Scheduling and Report service is not running, it will be restarted, and administrators alerted. If a report is not generated within a given time, all essential components will be re-initialized, pending Report Tool processes will be terminated and email notification is sent out Administrators.

Protection of Audit Information

Protect audit information and audit tools from unauthorized access, modification and deletion.
Allow restricted access to specific report collections

You need to …	Track & Audit Features
Protect audit information by storing it in a physically separate repository.	Choose where Track & Audit stores the Repository. Set a specified path on a local or external drive or configure access to a password protected network drive.
Restrict access to audit records and tools by assigning Administrator or User roles.	Role delegation for audit configuration and review. Access is password protected. Only Administrators can access all Audit Reports and configurations.
Allow a user access to the Audit Reports they require.	In Track & Audit, set up server access and dedicated reports for a given user. They will only be able to view reports generated for them.
Unify access control via Active Directory.	Track & Audit can connect to Active directory to authenticate user access with their domain/Windows login details.