Transition from Secure Cloud Analytics to Cisco XDR

Contents

The key change

The Secure Cloud Analytics user experience will no longer be available on October 24, 2026. Cisco XDR becomes the operating interface for SCA-derived detections, investigations, asset context, notifications, exports, and related workflows.

Caution: The dedicated SCA-to-XDR customer transition program is scheduled to close on September 30th, while October 24, 2026, remains the target date for the planned deprecation of the SCA user interface. Activate Cisco XDR now so your team can complete the readiness actions described below.

Immediate actions and critical dates

What is happening, and what should I do now?

Status	Action required
Details	Cisco is retiring the SCA user experience and moving SCA-derived capabilities into Cisco XDR. Telemetry and analytics become part of broader XDR workflows for Activities, Detections, Incidents, Investigate, asset context, response, and automation.

Customer action	Activate XDR, connect the SCA tenant, validate access, use XDR Detections and Incidents for daily operations, use Activities for source telemetry cutovers, test XDR workflows, and export historical information before October 24, 2026.

What dates should I plan around?

Date	Milestone	What this means
September 15, 2026	AWS and Azure configuration setup for selected customers	Affected US and EMEA customers move to the recommended XDR configuration method.
September 30, 2026	Dedicated SCA-to-XDR customer transition program closes	Complete entitlement, provisioning, and readiness actions before the program closes.
October 7, 2026	AWS CloudTrail, Azure Activity Log, and GCP Audit Log detections cut over	Operate these sources in XDR.
October 14, 2026	Custom Event detections cut over; Incident Tuning, Watchlists, and Entity Groups configuration available in XDR	Move related workflows and configurations to XDR.
October 21, 2026	NetFlow detections cut over	Operate NetFlow detections in XDR.
October 24, 2026	SCA user experience no longer available	Complete the move to XDR and export historical data before this date.

What happens if I do nothing or have not provisioned XDR?

Status	Not recommended
Details	If you do not activate and connect Cisco XDR before the SCA user experience is removed, you will lose access to SCA and will not have the replacement XDR experience available for your SCA-derived workflows, detections, investigations, integrations, or historical data. Waiting also compresses activation, user setup, workflow validation, and operational change into the final part of the transition.
Customer action	Activate and connect XDR now so your team can complete user setup, workflow validation, and export preparation before September 30, 2026. The SCA interface remains targeted for deprecation on October 24, 2026; without a connected XDR tenant, there is no replacement XDR experience available when SCA access ends.

What is retiring, changing, or not available

Which SCA concepts are explicitly not continuing in the same form?

Status	Change or retirement
Details	• SCA user experience: removed October 24, 2026. • Legacy SCA webhook behavior: replaced by XDR workflows. • SCA Observation experience: not a one-to-one XDR feature. • Subnet sensitivity: replaced by asset-value prioritization concepts. • Entity groups: replaced by asset labels, asset groups, and value scoring. • Snoozed detection settings: not migrated; use Incident Tuning when available. • Customer-controlled alert priority behavior: not retained.

	• Some reporting, lower-usage pages, and functions: retired or replaced by XDR-native experiences.

Which reporting or integration items are expected to be deprecated or moved?

Status	Expected change
Details	Examples include cloud posture watchlist, Kubernetes monitoring, AWS visualization/dashboard/session-search/IP-search experiences, Meraki and Umbrella context integrations, and email-based monthly reports and daily alert summaries. This list does not promise a one-for-one replacement for each legacy page.

What is not being asked of me in this migration?

Status	No action of this type
Details	Cisco is not asking customers to redeploy existing network sensors, reconfigure cloud log ingestion solely for the UX migration, manually recreate supported standard detection configuration objects, or retain SCA as a long-term parallel console.

Customer readiness checklist

1. Activate Cisco XDR and connect the existing SCA tenant before September 30, 2026, so your team can complete readiness actions before the transition program closes.
2. Create users, validate sign-in, and confirm appropriate access in XDR.
3. Review Detections, Incidents, Activities, Investigate, and Asset Insights / Device Insights.
4. Map every SCA webhook, export, notification, SIEM/SOAR handoff, and custom automation to XDR workflows or another XDR operating surface.
5. Validate required source telemetry in Activities as each source becomes available.
6. Validate required detections and response playbooks before each source cutover.
7. Review subnet sensitivity, entity groups, Snooze, alert priority, Watchlists, scanner rules, trusted networks, and asset-value prioritization.
8. Inventory legacy reports, SCA-only pages, and API dependencies; identify alternatives or export requirements.
9. Export required Alerts, Observations, raw logs, configuration records, and reports before October 24, 2026.

Finding your way in the new XDR experience

Are SCA customers entitled to Cisco XDR?

Status	Available as part of transition
Details	Existing SCA customers are entitled to Cisco XDR as part of the transition. The intended outcome is continued SCA value while core workflows move into XDR.
Customer action	Activate Cisco XDR, connect the existing SCA tenant, and use the Cisco XDR activation process if assistance is required.

Where do my SCA functions land in Cisco XDR?

SCA function	XDR destination
Alerts and alert workflows	XDR Detections and Incidents
Observations and event-oriented investigation	XDR Activities and XDR Investigate
Event Viewer	XDR Investigate and Activities
Device context	Asset Insights / Device Insights
Webhooks, notices, exports, and downstream delivery	XDR workflows
Detection configuration	XDR configuration experiences as each setting reaches its milestone

Will SCA remain available as a parallel daily-use console?

Status	No
Details	The SCA user experience is scheduled to be removed on October 24, 2026. Use the overlap period to practice the XDR operating model, validate workflows, and update runbooks.

Detections, incidents, and observation use cases

Are detections simply moving one-for-one?

Status	Model change
Details	No. Cisco is evolving detection content and the operating model rather than copying every legacy SCA alert as an unchanged XDR object. Names, logic, evidence, correlation, and outcomes can change.
Customer action	Evaluate the XDR detection outcome, evidence, and incident correlation against the security scenario you need to operate; do not use name matching alone as acceptance.

Should I use XDR Incidents or Detections for my alert workflow?

Status	Choose by outcome
Details	Use Incidents for human response, analyst notifications, triage, escalation, case management, and coordinated response. Use Detections for individual findings, detection-level exports, and machine-to-machine automation. Activities is the telemetry surface.
Customer action	Update runbooks so human notifications and response processes are triggered from Incidents where appropriate; use Detections for detailed analysis, exports, and finding-level automation.

Will observation-based use cases continue?

Status	Not one-to-one
Details	Do not assume the legacy observation name, UI object, or trigger condition will remain. The target is equivalent or improved coverage through Activities, Detections, Incidents, and broader correlation.
Customer action	Identify and update dependencies in runbooks, dashboards, and automation before October 24, 2026.

What if I rely mostly on NetFlow and cannot deploy EDR?

Status	Still in scope
Details	Existing network sensors and ingestion remain functional, and EDR deployment is not required to continue using migrated network detections.
Customer action	Use XDR Detections, Findings, Incidents, Incident Tuning, and available asset context. Request deployment-specific guidance if endpoint visibility is highly constrained.

Notifications, exports, webhooks, and automation

What happens to SCA webhooks?

Status	Migrate and test
Details	XDR Automate workflows are the long-term control point for notifications, exports, and downstream automation. The target export path is OCSF-aligned and can provide more complete contextual detection details than the legacy SCA Alerts and Observations model.
Customer action	If a webhook sends detection information to people, SIEM, SOAR, or another system, recreate and test that behavior in XDR workflows.

What is the difference between detection and incident workflows?

Status	Use the matching trigger
Details	Use detection-oriented workflows for data movement, exports, and machine consumption. Use incident-oriented workflows for broader operational activity and human notifications such as email, Slack, or Webex. Both can support exports.

What changes for SIEM, SOAR, or custom downstream integrations?

Status	Review required
Details	Do not assume an SCA-specific webhook, payload, alert name, or export will continue unchanged. The target export path is OCSF-aligned and can provide more complete and contextual detection details.
Customer action	Migrate dependencies to XDR workflows and the XDR data model, then test downstream receipt and runbook behavior.

Do I need to change NVM notifications and exports?

Status	NVM cutover completed
Details	NVM detections moved to XDR in May 2026. Customers relying on the legacy NVM webhook pattern needed to move notifications and exports to XDR workflows by the May 15, 2026 cutover.
Customer action	Continue to use and validate the XDR workflow pattern for NVM.

What should I test before a source cutover?

Status	Required readiness check
Customer action	For each source, test the detection or incident trigger, notification or export payload, downstream receipt, filtering or routing rules, and updated runbook response. Test before the source leaves the SCA experience.

Telemetry sources and source-by-source cutovers

When will telemetry be available in XDR Activities?

Date	Telemetry milestone	Customer action
August 19, 2026	ONA data telemetry in Activities	Begin reviewing ONA telemetry.
August 26, 2026	CTB data telemetry in Activities	Begin reviewing CTB telemetry.
September 16, 2026	AWS VPC Flow Logs, Azure Flow Logs, and GCP VPC Flow Logs in Activities	Begin reviewing cloud flow telemetry.
September 23, 2026	AWS source configuration in XDR	Use the XDR configuration experience where applicable.
September 30, 2026	AWS CloudTrail, Azure Activity Logs, and GCP Audit Logs in Activities	Begin reviewing audit-log telemetry.

Do I need to redeploy network sensors or reconfigure cloud log ingestion?

Status	No, not solely for UX migration
Details	Existing network sensors and cloud log ingestion remain functional during this phase and do not need to be redeployed or reconfigured solely because the user experience and detections are moving to XDR.
Important exception	Public IP addresses or endpoints used by sensors and integrations may change. Review firewall rules, proxy allowlists, and other network controls; Cisco will provide required XDR endpoint details before a configuration change is required.

When do source detections cut over?

Status	Source-specific schedule
Details	At cutover, telemetry and detections for that source are no longer available for use through the SCA user experience. • October 7, 2026: AWS CloudTrail, Azure Activity Log, and GCP Audit Log detections. • October 14, 2026: Custom Event detections. • October 21, 2026: NetFlow detections.

Settings, tuning, watchlists, and asset context

Will my detection configurations be migrated?

Status	Phased migration
Details	Supported standard configuration objects are expected to migrate as part of the broader detection-engine transition. NVM detection settings moved to XDR in May 2026; other settings transition as their capability becomes available.
Customer action	Do not manually recreate standard settings solely for the migration unless Cisco publishes a specific instruction for your deployment.

What replaces subnet sensitivity, entity groups, and Snooze?

Status	Concepts change
Details	• **Subnet sensitivity:** replaced by device value prioritization scoring in Asset Insights / Device Insights; scheduled in XDR Device Insights by September 30, 2026. • **Entity groups:** configuration scheduled in XDR Device Insights on October 14, 2026; existing groups migrate to Labels, with asset labels and value scoring used for prioritization. • **Snooze:** snoozed settings are not migrated; Incident Tuning is scheduled to become available on October 14, 2026.

When do Watchlists move?

Status	Scheduled October 14, 2026
Details	Watchlist configuration is scheduled to be available in XDR on October 14, 2026. Existing watchlists will be migrated, but terminology and rule presentation may change while the logic is preserved.
Customer action	Validate watchlist-dependent rules, suppression, and workflows during the transition.

Can I still set alert priority the way I did in SCA?

Status	No
Details	Alert priority is hard-set using Cisco threat research and is not a customer-managed false-positive suppression control.

Sensors, cloud integrations, and operational health

Will FTD, ISE, AWS, Azure, or GCP integrations remain unchanged?

Status	Validate business-critical paths
Details	Do not assume every integration retains the same UI, workflow, or configuration method. GCP configuration is already in XDR; AWS and Azure are moving next; on-premises sensor-related migration items move in October.
Customer action	Validate FTD, ISE quarantine, enrichment, SAL-connected workflows, and other business-critical integrations against product-specific guidance.

Can I monitor sensor health, liveness, flow delivery, and volume in the same way?

Status	Readiness review
Details	Cisco is maintaining sensor and ingestion operation during the transition, but not every SCA monitoring page or workflow is committed to migrate one-for-one.
Customer action	Inventory the health, protocol, flow-volume, and delivery checks you depend on and validate their XDR operating path.

Will ONA or CTB image distribution, destination URLs, service keys, or public IP

addresses change?

Status	Review network dependencies
Details	Cisco is not requiring sensor redeployment in this phase, but telemetry destinations may change as sources transition to XDR.
Customer action	Review firewall rules, proxy allowlists, destination URLs, and service-key dependencies before the relevant source cutover. Do not make preventive sensor changes without published migration instructions.

Historical data, reporting, and administration

What happens to historical SCA data when the SCA user experience turns off?

Status	Export before October 24, 2026
Details	Access to historical data through the SCA interface ends when the user experience is removed. Raw telemetry is ingested into XDR ahead of and through the detection migration path, but SCA is not the long-term location for historical retrieval. • Alerts and Observations can be exported as CSV from the SCA console. • Raw logs, including network traffic and cloud logs, can be exported as CSV if needed. • Define audit, forensics, and retention evidence requirements before exporting.

Will all SCA reporting functions move to XDR?

Status	Some retired or replaced
Details	Some reporting functions, lower-usage pages, and legacy functions are expected to be retired or replaced by XDR-native Detections, Investigate, Activities, and Asset Insights experiences.
Customer action	Inventory operationally required reports now and identify the XDR experience, export, or replacement workflow.

How should I demonstrate migration completeness?

Status	Define proof artifacts
Customer action	Define required records and evidence, export needed SCA history before October 24, 2026, and validate XDR visibility for each required source. The transition is not a customer-managed bulk reimport into a separate system.

What happens to administrator information stored on the SCA side?

Status	Document before decommissioning
Details	Do not assume that customer-visible configuration, administrative information, or history stored in SCA will remain available after October 24, 2026.
Customer action	Export or document anything required for administration, audit, or historical reference, and use XDR as the target operating interface.

APIs and custom integrations

What replaces the Get Observations API, SCA Devices API, or other SCA-specific APIs?

Status	Inventory dependencies
Details	Cisco has not published a final one-for-one API replacement matrix for every SCA API. Plan around Activities, Detections, Incidents, workflows, Asset Insights / Device Insights, and XDR Investigate.
Customer action	Inventory direct dependencies now and do not assume legacy endpoint names remain available after October 24, 2026.

What happens to legacy incident-creation methods and custom automation?

Status	Treat as transitional
Details	The FAQ does not establish a committed public deprecation date for every legacy incident-creation method or API. The target direction is XDR custom security events and detections, incident generation in the XDR model, and Incident Tuning for outcome management.
Customer action	Map every automation consuming SCA observations, alert names, devices, webhooks, exports, or reports to an XDR workflow, detection, incident, activity, or Asset Insights use case. Test end-to-end behavior before the relevant source cutover.

Completed transition items

NVM detection migration

Status	✅ Completed
Resolution	NVM detections and related detection settings moved into XDR in May 2026. Customers relying on legacy NVM notifications and exports should use XDR workflows and validate the workflow pattern.