

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Identity Intelligence Demystified

Technical deep dive into CII (formerly Oort)

Aaron T Woland, CCIE #20113

Distinguished Security Engineer

loxx@cisco.com |  aaronwoland |  aawoland

BRKSEC-2162

CISCO *Live!*

#CiscoLiveAPJC

\$ whoami



Cisco role: Distinguished Engineer,
Security

Unofficial title:
“Cisco History Professor”

Experience: Old enough to wonder how
I have been doing this for >30 years

Fun fact 1: Father of 5 daughters

Fun fact 2: Oldest works for Cisco now!
Youngest is 3!

Fun fact 3: Just completed Cybersecurity
Master’s Degree from SANS Institute
(Oct 2024)

Sarcasm

“If we can’t laugh at ourselves, Then we cannot laugh at anything at all”



Disclaimer: “All Comments are my own, and are not representative of Cisco... Any correlation to real live persons or situations was completely unintentional... Blah Blah Blah...”



Please fill out the survey



Drop your email in the comments – I WILL respond!

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

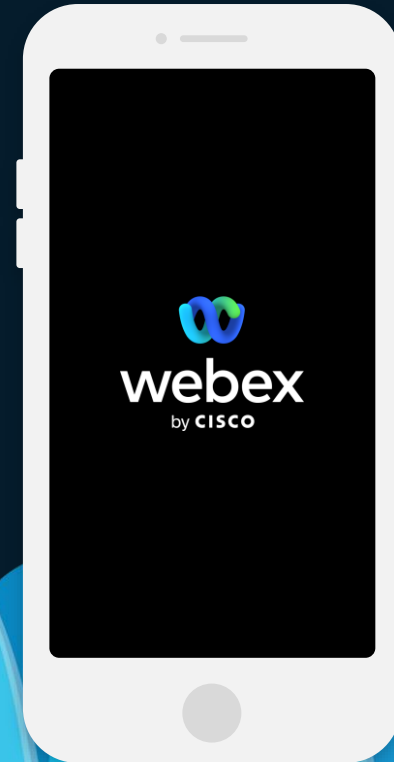
How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2162>





Agenda

- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- Let's talk about APIs
- Call to Action

Cisco Identity Intelligence



Users



Machines



Services



Apps



Data



Behaviors



Auth0

Workday

Okta

GitHub

Salesforce

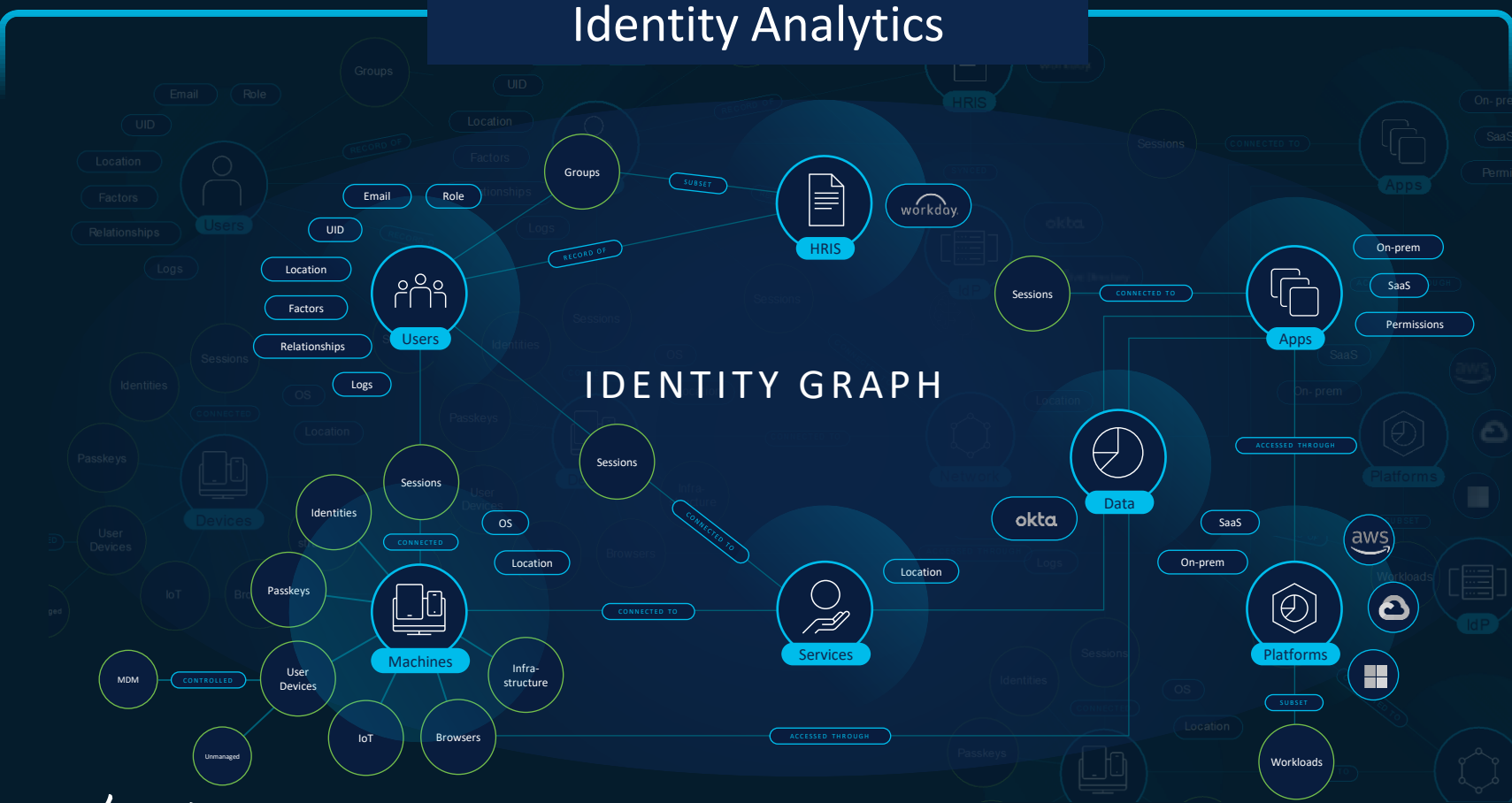
Microsoft



Google

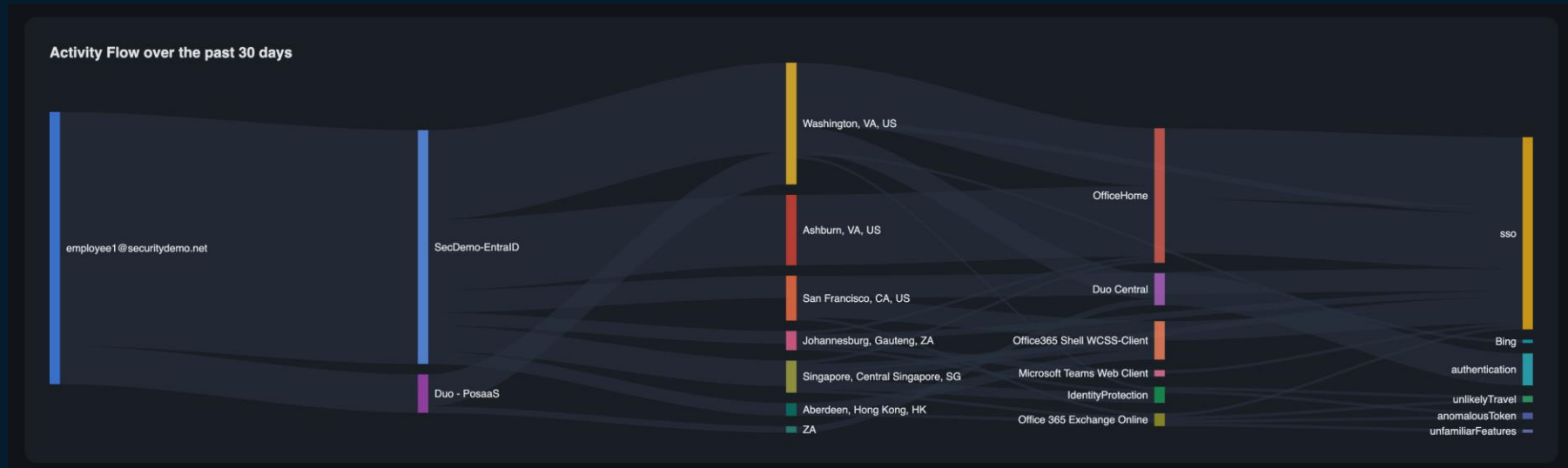
Amazon

Identity Analytics



Real life example of detection

Identity graph - Threat analysis based on probed account

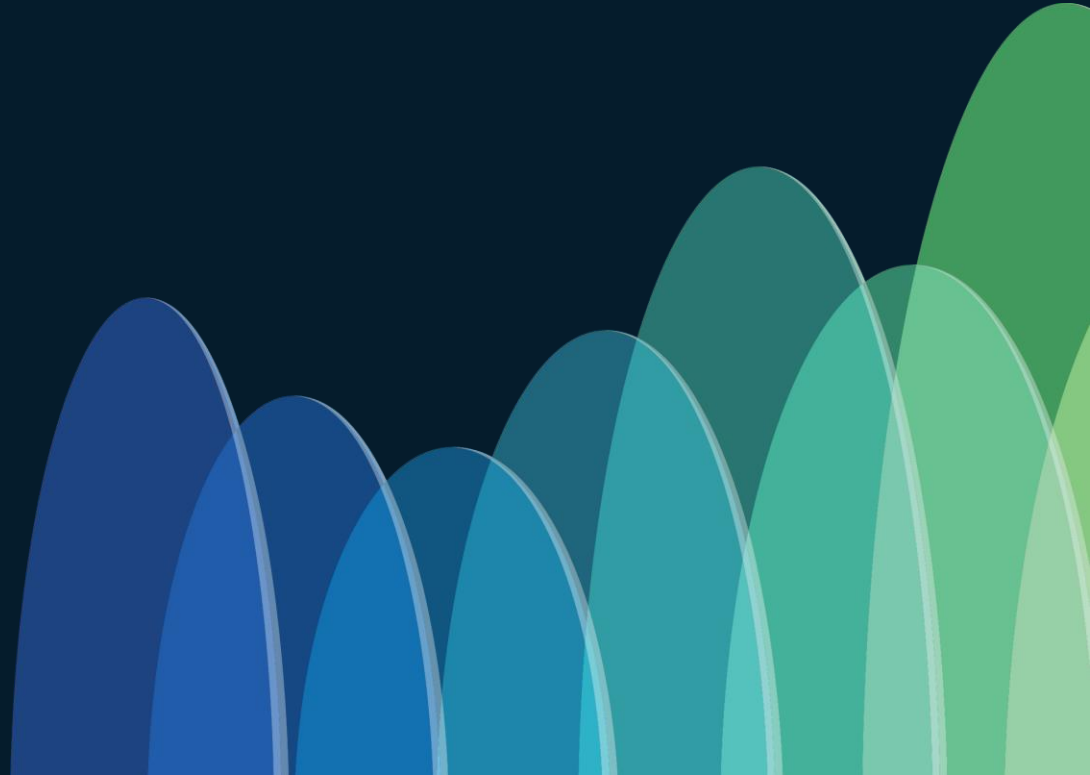




Agenda

- What is Cisco Identity Intelligence
- Integrations & Users
- All about Checks
- Remediations
- Other Technical Nuggets
- Let's talk about APIs
- Call to Action

Integrations Overview



Integrations are the life's blood of CII

Identity Providers

CII integrates w/ many key (cloud-based) ID sources already.

These integrations are complex in nature.

IM & Notification

Operational alerts and failed checks send to these integration targets.

Support of webhook destinations offers a standard interface for integrating CII to other systems.

API Clients

These are the client credentials for the public GraphQL API to query CII for information

Integrations

Providers

Name	Collection Status	Recent Usage	Average Traffic	Last Collected (UTC)	Last Updated (UTC)
Duo - PosaaS	✓ Success Traffic detected		12 records	Apr 12, 2024 14:26:55	Mar 29, 2024 16:42:04
Loxx-Oкта	✓ Success Traffic detected		15 records	Apr 12, 2024 14:26:53	Apr 2, 2024 16:13:08
SecDemo-EntralID	✓ Success Traffic detected		11297 records	Apr 12, 2024 14:27:55	Apr 2, 2024 13:08:22
Slack - SecurityDemo.Net	✓ Success Traffic detected		4 records	Apr 12, 2024 14:26:52	Apr 3, 2024 00:57:00
loxx.tv	✓ Success Traffic detected		5 records	Apr 12, 2024 14:56:54	Apr 3, 2024 00:42:05

Instant Messaging

Team	App
SecurityDemo.Net	Slack

Notification Targets

Name	Description	Type	Last Updated (UTC)
Aaron XDR Listener	Listener configured in XDR for webhooks	Check failures	Apr 12, 2024 18:40:15
SecurityDemoNet-Oort-Messages		Check failures	Apr 12, 2024 18:40:19
Securitydemo Slack		Check failures, Data collection	Apr 12, 2024 18:40:23

API clients

Name	Status	Client ID	Description	Last Updated (UTC)
Robins Toy Box API Client	✓ Enabled	xKivt6q2wErXx5ZqWSlibC-WX41ZF9		Mar 28, 2024 20:50:52
Aaron - API for XDR Dashboards	✓ Enabled	LHMtfeBUubrQVJ175zpSTOnNsYAlfSe		Mar 28, 2024 20:45:19

Data collection methods

- Identity Intelligence utilizes native REST APIs of all supported sources
 - **Full inventory sync** – an API call to the source which results in the download of the full user database of this source. Such calls are executed on the initial sync and later over long enough intervals to avoid exhausting the API subsystem of the source.
 - **Delta sync** – when possible, uses API calls that return only changed information. Timestamps like 'last updated' are used to identify what has been changed after the last full or delta sync.
 - **Streaming** – the most desired way of getting data! May use AWS EventBridge, or Azure Event Hub & the providers will send all notifications to CII in near-real-time based on the events we are subscribed to.
 - Streaming is always preferred. API's have rate limits and throttles.

Identity sources and their methods

Identity Sources	Streaming	REST API Full Sync	REST API Delta Sync
Duo Security by Cisco	✓	✓	✓
Microsoft Entra (aka: Azure)	✓	✓	✓
Okta	✓	✓	✓
Slack ¹	✗	✓	✓
Github	✗	✓	✓
AWS	✗	✓	✓
Google Workspace	✗	✓	✓
Workday	✗	✓	✗
Salesforce	✗	✓	partial
Auth0 (acquired by Okta)	✓	✓	✗
Manual Upload (CSV/JSON)	✗	✗	✗

¹ listed as notification, but also an identity source

Wait... Why not just use the IDP?

- Okta, Microsoft – they all claim to provide ID security!
 - But they can only detect what they see!
 - Most organizations have multiple IDPs, correlation is very difficult
- CII brings together the info!
 - All factors together in one analytical system
 - Greatly reduces the noise from the IDPs
 - Reducing false-positives
 - Proactive & Reactive Security
 - Work closely with Okta, MSFT & Duo to develop features together

“CII gets great insights from Entra, and I cannot believe how bad Entra is at using their own alerts”
- Fortune 100 Manufacturing Co

Merged view of users – combined from all sources

Merged Users

The user inventory is built out based on the users from each provider. When the user is the same across multiple providers, those users are merged for a combined view.

Usually see a 20-30% difference between what an organization *thinks* they have vs. what they *actually* have.

The screenshot displays the Cisco Identity Intelligence interface. On the left, a sidebar contains various filters. The 'Sources' filter is expanded, showing a list of providers: Duo - PosaaS (17), Loox-Okta (17), SecDemo-EntraID (17), Slack - SecurityDemo.Net (1), and others. An orange box highlights this 'Sources' filter. The main area shows a table of 17 users found. The table has columns for User, Checks, # IPs, # Logins, Last Seen (UTC), Last IP Address, Last Location, MFA, Providers, and Status. An orange box highlights the 'Providers' column, which shows icons for each provider associated with the user. The users listed include Chris Murray, Derrick Snider, Donald Duck, Employee2, EmployeeOne, Loox, Matt Vander Horst, Patrick Cardot, and Paul Carco.

User	Checks	# IPs	# Logins	Last Seen (UTC)	Last IP Address	Last Location	MFA	Providers	Status
Chris Murray chris@securitydemo.net	✓	2	1	8 Days Ago Apr 3, 2024 15:29:35	84.71.178.25	Harrow, England, GB	✓	[Duo] [Okta]	Active
Derrick Snider dersnide@securitydemo.net	1	2	1	7 Days Ago Apr 4, 2024 13:44:25	136.62.139.21	Austin, TX, US	✗	[Duo] [Okta]	Active
Donald Duck donald_duck@securitydemo.net	1	0	N/A	N/A	N/A	N/A	✗	[Duo] [Okta]	Active
Employee2 employee2@securitydemo.net	1	1	N/A	A Month Ago Mar 14, 2024 16:35:09	171.68.244.70	San Jose, CA, US	✗	[Duo] [Okta]	Active
EmployeeOne employee1@securitydemo.net	1	9	30	A Day Ago Apr 10, 2024 20:52:45	54.91.54.189	Ashburn, VA, US	✓	[Duo] [Okta]	Active
Loox loox@securitydemo.net	2	17	94	4 Hours Ago Apr 11, 2024 16:19:01	75.182.151.17	Waxhaw, NC, US	✓	[Duo] [Okta]	Active
Matt Vander Horst matt@securitydemo.net	1	3	25	6 Days Ago Apr 5, 2024 15:42:48	71.234.238.50	South Hadley, MA, US	✓	[Duo] [Okta]	Active
Patrick Cardot pcardot@securitydemo.net	1	2	1	A Day Ago Apr 10, 2024 20:03:30	37.65.38.86	Douchy-les-Mines, Hauts-de-Fra...	✗	[Duo] [Okta]	Active
Paul Carco carco@securitydemo.net	2	4	7	2 Days Ago Apr 9, 2024 20:35:01	173.38.117.65	Cary, NC, US	✓	[Duo] [Okta]	Active

Users

User 360 View

The user details is known as the “user 360 view”

A true look at the user’s identity related security, activity and other important properties.

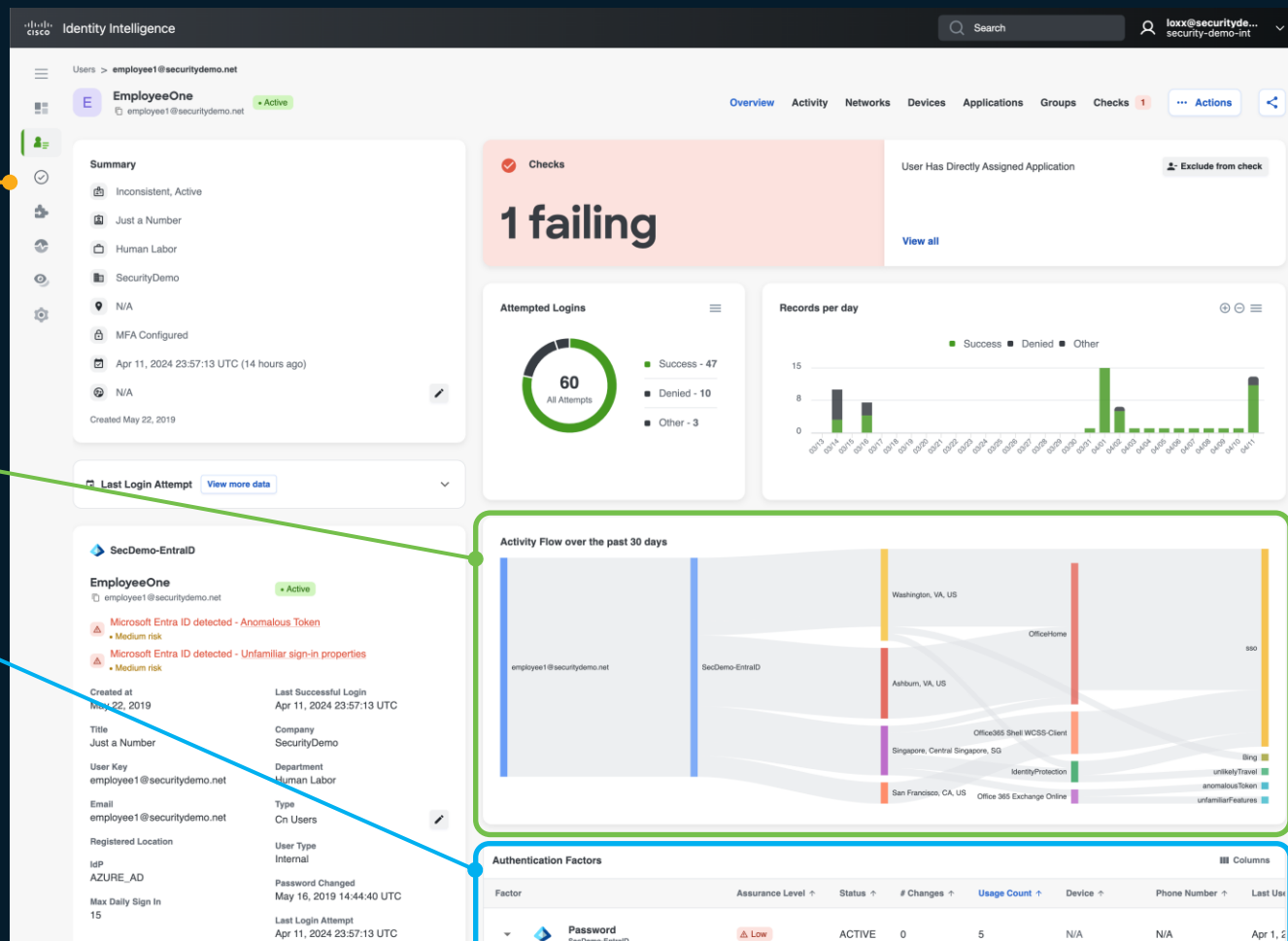
Activity Flow

Combined view of the user's activity patterns. Easily spot when deviations have occurred

Combined Auth Log

Combined view of the users authentications and factors across all the integrated IdPs

CISCO *Live!*



Activity

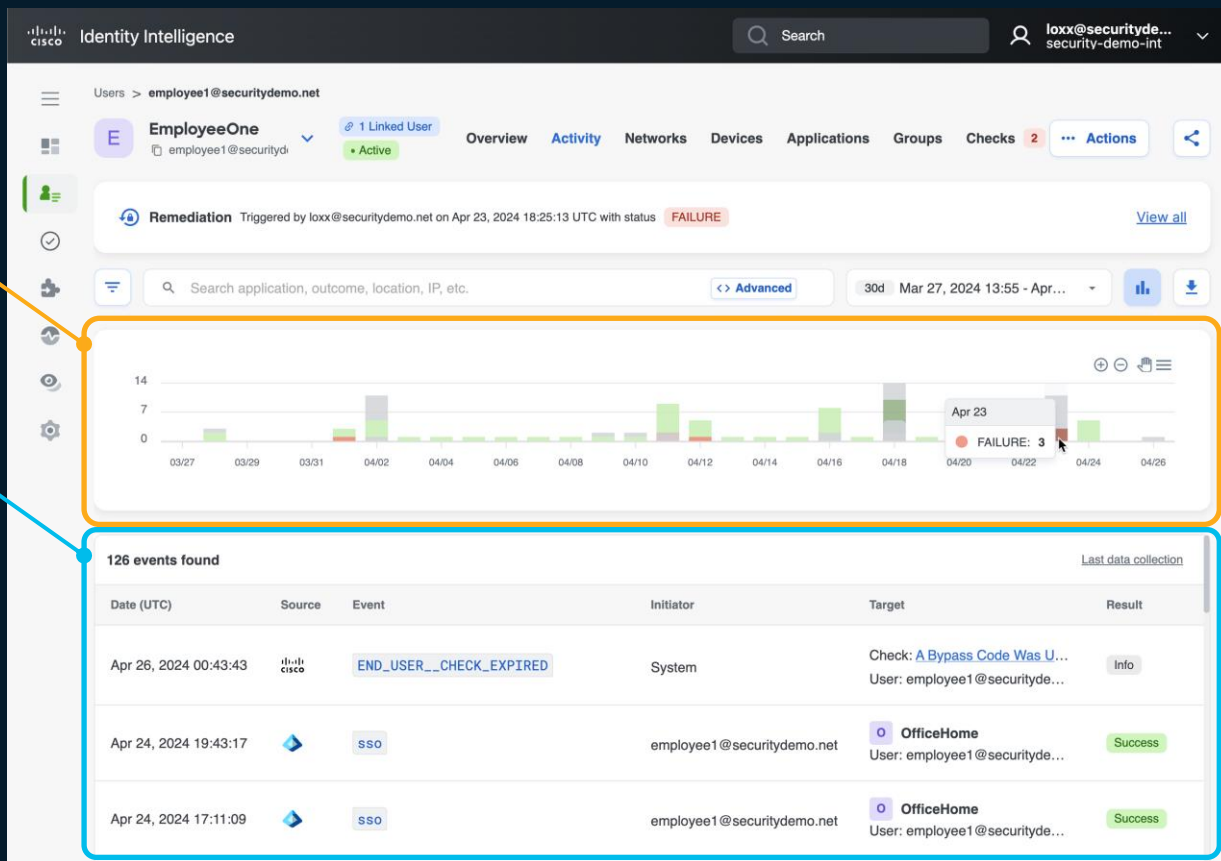
Activity Timeline

See the authentication trends across the timeline.

Zoom in & out.

Activity List

See the login activity, and click in for progressive-disclosure all the way to the detailed raw-logs



Networks

IP's recorded in IDP Logs

These are not the "internal IP's".
These are the source IP's when the
user-agent communicated to the IDP
during auth flow

Locations

Do these seem normal for the user?

Is this suspicious?

The screenshot shows the Cisco Identity Intelligence interface for a user named 'employee1@securitydemo.net'. The 'Networks' tab is selected, displaying a table of 14 IP addresses. A blue box highlights the table, and a red box highlights the location information for the IP 85.203.21.87, which is 'Singapore, Central Singapore, ...'. A red line points from the text 'Do these seem normal for the user?' to the location information. A blue line points from the text 'IP's recorded in IDP Logs' to the IP address column.

IP Address	Last Access (UTC)	Hit Count	Successful Events	Failed Events	Other Events	Tags	Location
54.91.54.109	Apr 25, 2024 19:38:19	24	24	0	0		Ashburn, VA, US
172.203.228.226	Apr 18, 2024 17:50:41	18	10	1	7		Washington, VA, US
20.51.250.58	Apr 24, 2024 17:11:09	14	10	4	0		Washington, VA, US
128.107.78.71	Apr 12, 2024 00:08:15	7	7	0	0		San Francisco, CA, US
85.203.21.87	Apr 12, 2024 07:00:56	5	2	3	0		Singapore, Central Singapore, ...
154.16.95.37	Apr 20, 2024 02:47:10	3	2	1	0		Johannesburg, Gauteng, ZA
193.176.211.235	Apr 16, 2024 15:09:57	3	3	0	0		Aberdeen, Hong Kong, HK
154.16.95.18	Apr 18, 2024 19:17:42	1	0	1	0		ZA

Devices

Devices from IDPs

Not all IDPs are created equal with device information

Duo is the best source for device data – when the Duo Auth includes the Health App.

Standard IDP would only see the user-agent string, no real device information.

List includes MFA devices and access devices.

Device starts with “EP”

These are the Duo Epkeys, a secure-cookie used to identify a user+device pair.

EmployeeOne | 1 Linked User | Active

Overview | Activity | Networks | **Devices** | Applications | Groups | Checks | 2 | Actions

Remediation Triggered by loxx@securitydemo.net on Apr 23, 2024 18:25:13 UTC with status **FAILURE** [View all](#)

14 devices found

Device	Source	OS	Managed	Registered	Usage Count	Enrolled (UTC)	Last Seen (UTC)
Access and Authentication devices							
EPJPCXC18SO57X3G4J0G	Duo - PosaaS	iOS 15.7	✗	✓	N/A		
EPTFXOBY41570W7UW9OR	Duo - PosaaS	iOS 16.7.6	✗	✓	N/A		
EPWQ1HG7NCQ5UYST8BR5	Duo - PosaaS	iOS 16.7.6	✗	✓	N/A		
AAWOLAND-M-W1J9	Duo - PosaaS	Mac Os 14.3.1	✓	✓	N/A		
ATW-LABSTINKPAD	Duo - PosaaS	Windows 10.0.19044.2728	✓	✓	N/A		
MJOHARI-M-2XK7	Duo - PosaaS	Mac Os 14.3.1	✗	✓	N/A		
SSAKLIKA-M-X2WT	Duo - PosaaS	Mac Os 14.3.1	✓	✓	N/A		

Applications

Usage Statistics

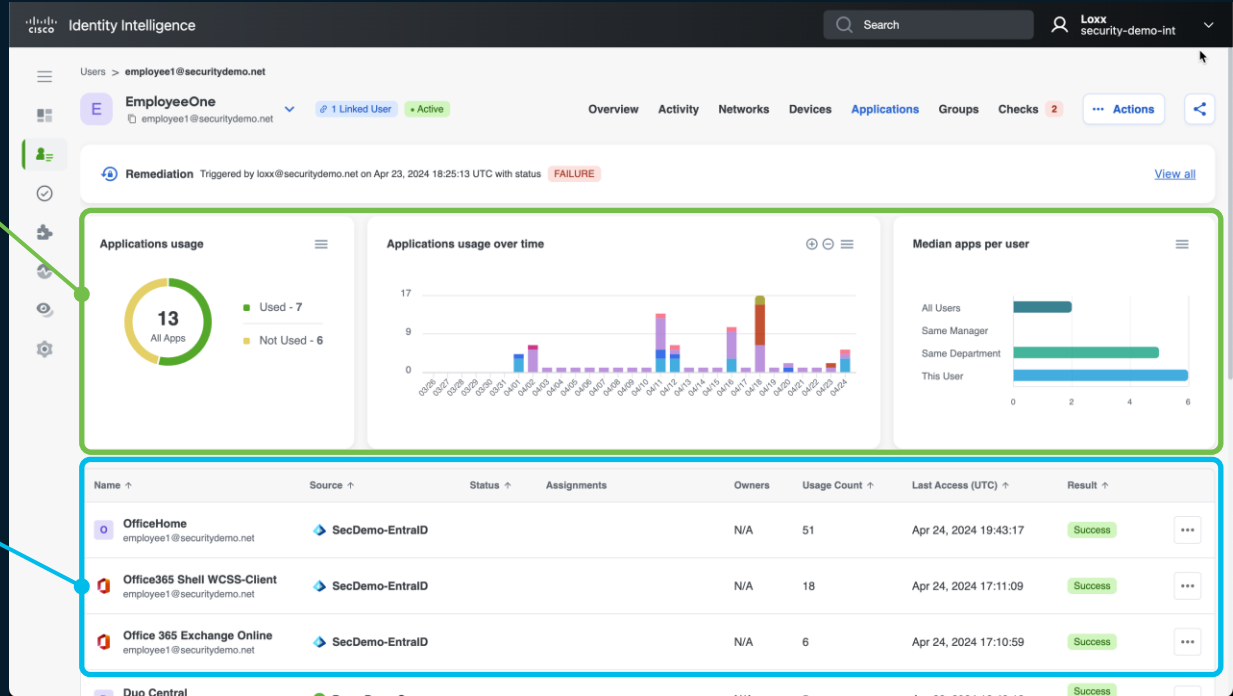
Quick overview of the apps used

Includes Apps not used

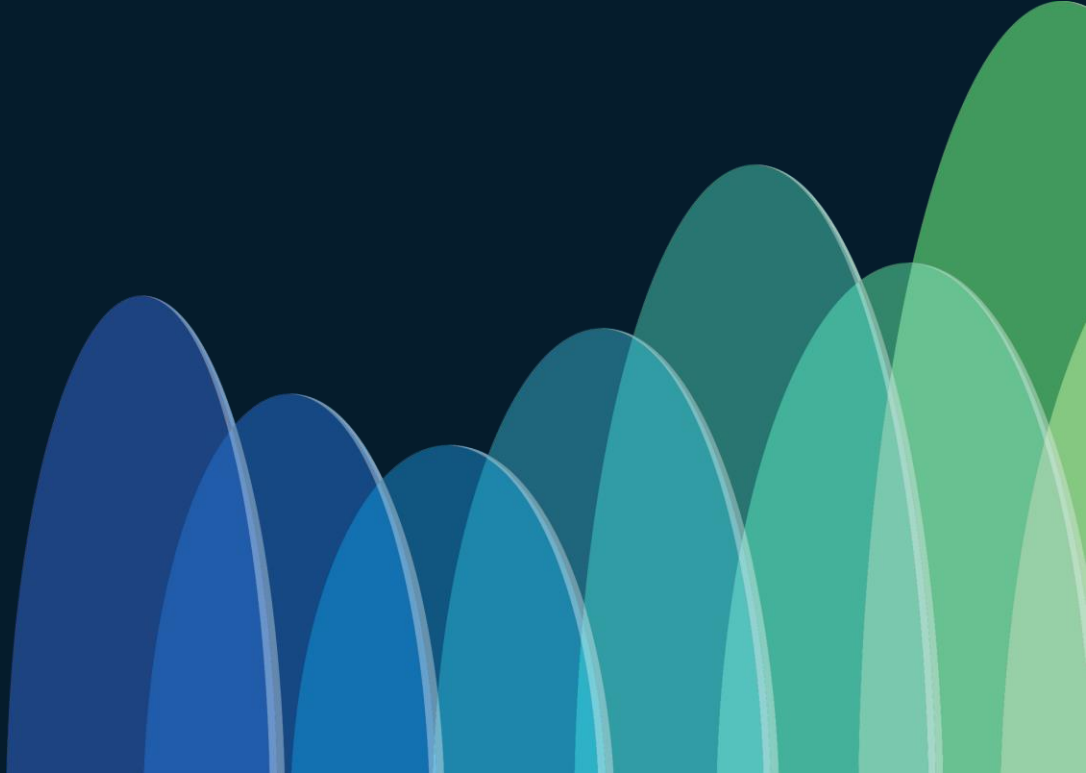
Application List

Which applications is the user accessing (according to the IDPs).

Which IDP reported the access & usage counts.



Integrations Deep Dive



Excellent Documentation

- All integrations have a detailed guide to go along with them
 - They will have links to the 3rd party vendors pages for specific sections of the integration
- Keeps the CII documentation up to date, and puts the ownership of that portion on the vendor directly

The screenshot shows the Oort Knowledge Base interface. On the left is a navigation menu with links to Home, Glossary, Best Practices, How-to Guides, Oort Insights, and Integrations. Under Integrations, there is a list of integration guides, with 'Microsoft Entra ID (Azure AD) Data Integration' highlighted in blue. The main content area on the right displays the title 'Microsoft Entra ID (Azure AD) Data Integration' with a date of '11/2023'. Below the title is an 'Overview' section explaining that Oort's platform analyzes authentication events in Microsoft Entra ID to provide insights into user access. It also mentions that the document will guide the user through setting up API access and integrating with the Oort console. An 'Important Notes' section follows, containing two bullet points: one about SSO integration and another about new tenants. A 'Next Steps' section states that once integration is complete, a review will be conducted. The 'Entra ID Integration' section begins by stating that Entra ID has different activity log types. At the bottom of the page, it says 'Powered by GitBook'.

Oort Knowledge Base

Search

Home

Glossary

Best Practices

How-to Guides

Oort Insights

Integrations

Auth0

Microsoft Entra ID (Azure AD) Data Integration

Microsoft Entra ID (Azure AD) SSO Integration

Azure Event Hub Log Streaming for Microsoft Entra ID (Azure AD)

Azure Sentinel SIEM Integration

AWS

Duo Security Integration

GitHub

Google Workspace Integration

Jira Integration

Mailgun Integration

Microsoft Teams Notification Integration

Okta Log Streaming AWS EventBridge Integration

Okta Data Integration

Okta Workflows

Integration Marketplace

Powered by GitBook

Microsoft Entra ID (Azure AD) Data Integration

11/2023

Overview

Oort's platform can analyze authentication events in Microsoft Entra ID (Azure AD) to give insights into how users are accessing your applications. In order to provide Insights, you have to set up an integration between Microsoft Entra ID and Oort for analysis. This document will walk you through the process of setting up API access inside of Entra ID and will also walk you through the complementary set up inside of the Oort console.

Important Notes

- This integration is for Entra ID data collection. For SSO to your Oort tenant using Entra ID, please see [Microsoft Entra ID \(Azure AD\) SSO Integration](#)
- If this is a brand new Microsoft Entra ID tenant, for instance a development environment, then make sure to enable a Microsoft Entra ID subscription and resource provider.

Next Steps

Once the integration is complete and the Oort platform has completed the analysis of the data, Oort will set up a review with you and your team to share insights discovered through the integration.

Entra ID Integration

Entra ID has different activity log types which each contain different sets of information. Oort

View Logs

The screenshot shows the Cisco Identity Intelligence 'Integrations' page. It lists several providers with their respective collection statuses and usage metrics. A dropdown menu is open for the 'Duo - PosaaS' provider, highlighting the 'View Logs' option with a blue arrow.

Name	Collection Status	Recent Usage	Average Traffic	Last Collected (UTC)	Last Updated (UTC)
Duo - PosaaS	Collecting View Logs	[Line graph]	13 records	Apr 18, 2024 19:27:50	
Loxx-Okta	Success Traffic detected	[Line graph]	22 records	Apr 18, 2024 19:26:53	
SecDemo-EntralD	Collecting View Logs	[Line graph]	18259 records	Apr 18, 2024 19:26:53	
Slack - SecurityDemo.Net	Success Traffic detected	[Line graph]	7 records	Apr 18, 2024 19:26:53	Apr 3, 2024 00:57:00
loxx.tv	Success Traffic detected	[Line graph]	5 records	Apr 18, 2024 18:57:09	Apr 3, 2024 00:42:05

Ellipses (...)

- Edit Settings
- Test connectivity – Terrific way to ensure the connection is working as expected
- Trigger collection (sync)
- Disable collection - use when there is an issue, and then enable again after that issue is resolved
- [View Logs](#) – see all logs related to the specific integration.
- Delete

View Logs

Integration Logs

Built into the UI, it will automatically filter and display all logs related to the integration, its syncs and any other related information.

You can click in & leverage progressive disclosure to view the raw log, too.

The screenshot shows the Cisco Identity Intelligence 'System Logs' interface. On the left, a sidebar contains filter sections: 'Result' (Blocked, Failure, Info, None, Partial success, Started, Success, Timeout), 'Event Family' (Integrations, User checks, Admin triggered), and 'Check Actions Taken'. A red arrow points to the 'Event Family' section. The main area displays a table of 1722 events. The table has columns: Date (UTC), Event, Initiator, Target, Result, and Logged By. The events are filtered by 'Target: Duo - PosaaS'. The table shows a list of events, mostly with 'Success' results, and one event with an 'Info' result.

Date (UTC)	Event	Initiator	Target	Result	Logged By
Apr 18, 2024 19:28:00 Ended in 0h 0m 1s	INTEGRATION__HISTORICA...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:28:00 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:59 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:59 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:57 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:56 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:53 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:52 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:50	INTEGRATION__COLLECTION	System	Duo - PosaaS	Started	cnt-integration
Apr 18, 2024 19:27:49 Ended in 0h 0m 0s	Mutation__triggerDataC...	loxx@securitydemo.net admin	Duo - PosaaS	Info	cnt-integration
Apr 18, 2024 19:27:02 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:02 Ended in 0h 0m 2s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:27:02 Ended in 0h 0m 3s	INTEGRATION__DATA_UPLO...	System	Duo - PosaaS	Success	cnt-integration
Apr 18, 2024 19:26:42 Ended in 0h 0m 50s	INTEGRATION__EVENTS__C...	System	Duo - PosaaS	Success	cnt-integration

Sync Schedule

- Manually Collect on Demand
- Also triggers a detection run when the collection is completed

The screenshot shows the Cisco Identity Intelligence 'Integrations' page. It lists several providers with their collection status, recent usage, average traffic, and last collected/updated times. A red arrow points to the 'Collect Now' option in the context menu for the 'Slack - SecurityDemo....' provider.

Name	Collection Status	Recent Usage	Average Traffic	Last Collected (UTC)	Last Updated (UTC)
Duo - PosaaS	Collecting View Logs		3 records	Jun 1, 2024 22:14:51	Apr 22, 2024 13:37:22
Loxx-Oкта	Success Traffic detected		13 records	Jun 1, 2024 21:26:53	Apr 29, 2024 01:51:30
SecDemo-EntraID	Success Traffic detected		33139 records	Jun 1, 2024 21:27:11	Apr 29, 2024 01:51:30
Slack - SecurityDemo....	Success Traffic detected		13 records	Jun 1, 2024 21:27:11	Apr 29, 2024 01:51:30
loxx.tv	Success Traffic detected		0 records	Jun 1, 2024 21:56:11	Apr 29, 2024 01:51:30

Context Menu for 'Slack - SecurityDemo....':

- Edit Settings
- Test Connectivity
- Collect Now
- Disable Collection
- View Logs
- Delete

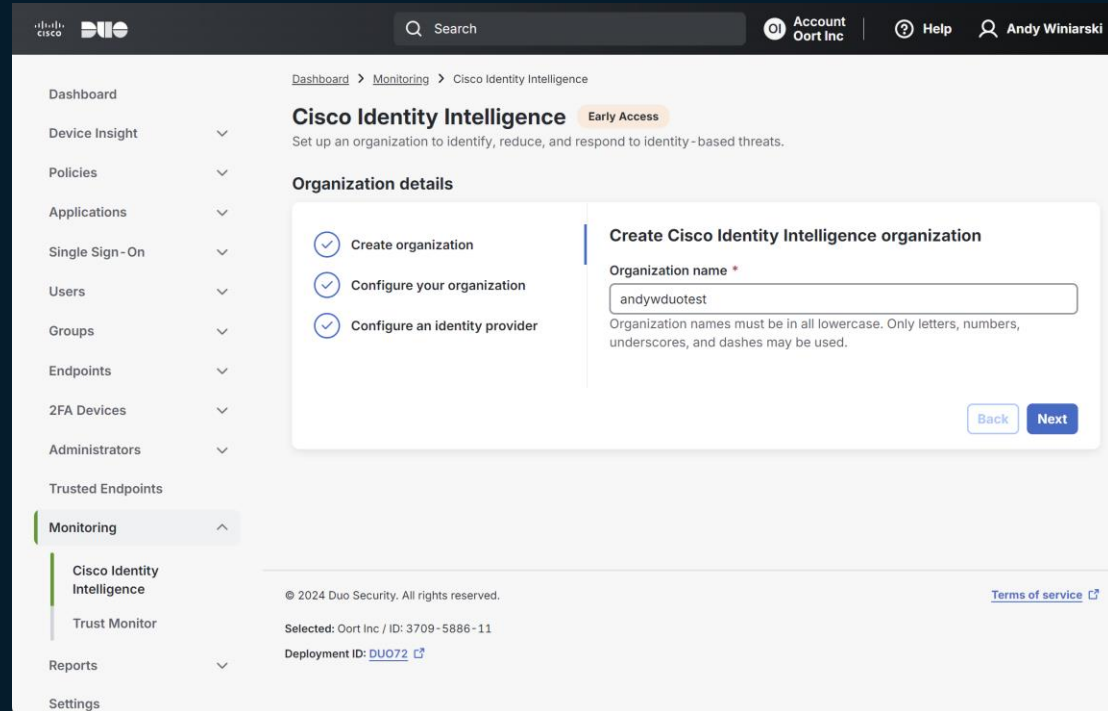
Duo

a Cisco Company



Duo <> CII Integration

- 3-step wizard to create and configure your CII tenant
 - Automatically integrates Duo data
 - Duo SSO setup or 3rd party SSO via OIDC
- All new CII trials will flow through the Duo/CII tenant provisioning



Duo and Identity Intelligence's Bright Future

- Duo has plans to use Identity Intelligence natively
- Failed checks in CII will influence the Risk Based Auth in Duo.
- Duo will expose the combined CII data within the Duo dashboard interface
- We're just getting started!

The screenshot shows the Duo Identity Intelligence dashboard for user Armstead Barton. The interface includes a sidebar with navigation options like Dashboard, Device Insights, Policies, Applications, Single Sign-On, Users, Groups, Endpoints, 2FA Devices, Administrators, Trusted Endpoints, Trust Monitor, Cisco Identity Intelligence, Reports, Accounts, Billing, and Settings. The main content area displays user information, authentication success rate (98%), active sessions (4), and vulnerabilities (3). It also features tables for Sources, Applications, Authentication Factors, and Authentication History.

User Information

Field	Value
NAME	Armstead Barton
EMAIL	armsteadbarton@acme.com
CREATED	May 7, 2018 9:30 AM (EDT)
MFA	Active

Authentication Success Rate

98%
15% Past 7 days

Active Sessions

4
Linked to this identity

Vulnerabilities

3
Linked to this identity

Sources

Source	Status	Weak MFA Was Used To Successfully Sign In
Duo	Active	Weak MFA Was Used To Successfully Sign In
Okta	Active	Weak MFA Was Used To Successfully Sign In
Azure AD	Active	Weak MFA Was Used To Successfully Sign In

Applications

Applications allowed	Applications not used
12	5

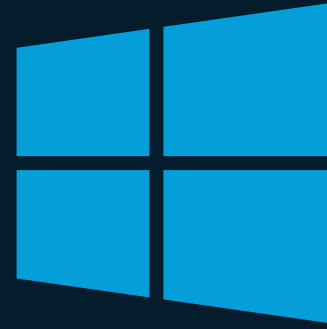
Authentication Factors

Source	Strength	Factor	Changes	Usage Count	Device	Phone Number	Last Used (UTC)
Azure AD	Weak	Phone	0	1	+1 2222222222	+1 2222222222	Nov 11, 2023 23:57:41
Azure AD	Weak	Password	0	0	N/A	N/A	N/A

Authentication History

Timestamp	Result	Application	Trust assessment	Access device	Authentication method
6:16:23 PM Feb 13, 2023	Granted	Web SDK	N/A	Mac OS X 10.15.7 Reported by Device Health	Duo Push United States
6:16:23 PM Feb 13, 2023	Denied	Web SDK	N/A	Mac OS X 10.15.7 Reported by browser	Unknown
6:16:23 PM Feb 13, 2023	Enrolled	Web SDK	N/A	Lastpass-1qs, Chantilly, VA, United States, 70168131229, Endpoint trust is unknown because there are no active Trusted Endpoints Configuration	Duo Push United States

Microsoft Entra ID



Aka: Azure Active Directory (AAD)

MS Entra ID

- All integrations w/ Azure go through an “App registration”
- That’s where you configure & get the API keys
- The “app” is given explicit or delegated permissions to a very granular set of controls / API

The screenshot shows the Microsoft Azure portal interface for App Registrations. The top navigation bar includes the Microsoft Azure logo, a search bar, and user information. The main heading is "App registrations". Below this, there are tabs for "New registration", "Endpoints", "Troubleshooting", "Refresh", "Download", "Preview features", and "Got feedback?". A notification banner states that starting June 30th, 2020, new features for ADAL and Azure Active Directory Graph will no longer be added, and applications will need to be upgraded to MSAL and Microsoft Graph. Below the notification, there are tabs for "All applications", "Owned applications" (selected), and "Deleted applications". A search bar prompts the user to "Start typing a display name or application (client) ID to filter these r...". Below the search bar, it says "4 applications found". The table below lists the applications:

Display name	Application (client) ID	Created on	Certificates & secrets
 Cisco XDR	3891ab18-5d91-4960-a5e6-bc24...	7/23/2021	✓ Current
 Kenna Integration	1b6aa786-ba19-43f5-821b-6d141...	1/9/2024	✓ Current
 Oort	07ef51a6-8052-4cc4-a5d8-dedaa...	6/15/2023	✓ Current
 SecureX Inventory Integration - Delete Me	fdceec30-bdc6-46f6-afa3-265f95...	3/22/2021	✓ Current

MS Entra ID

Event Streaming

Here you add the Event Hub that you created in Azure, to stream the events to CII.

It is not a true stream like Event Bridge in AWS offers, but it's close.

Event Hub will collect the events that CII has subscribed to & CII will pull those events on a schedule (15 minute intervals)

Identity Intelligence

Search

loxx@securityde... security-demo-int

Integrations > Edit Settings

Edit Microsoft Entra ID Settings

General Settings **Event Streaming** Advanced Settings

☒ Use EventHub for Logs Streaming

EventHub Name
loxx-cii-

Consumer Group
\$Default

Endpoint FQDN
servicebus.windows.net

Shared Access Key Name
ListenPolicy-Loxx

[Reset Credentials](#)

Cancel Save

Where can I see a step by step configuration guide? ^

Refer to [this documentation article](#) for a step by step guidance.

Are Directory ID and Tenant ID the same thing? v

Where do I get my Application ID? v

How do I get my Application Secret Value? v

© 2024 Identity Intelligence

This environment reloads hourly

[Privacy Policy](#) [Terms of Use](#) [Documentation](#) [SOC2 Report](#)

MS Entra ID

Advanced Settings

This is where you can tune which information CII should pull when performing sync's with Azure / Entra ID.

Some of the data types require Azure P1 or Azure P2 subscriptions, and CII leverages the information tool-tip to call those out.

Identity Intelligence

Search

Integrations > Edit Settings

Edit Microsoft Entra ID Settings

General Settings Event Streaming **Advanced Settings**

Data Types

Check all of the data types you want this integration instance to get. You can update this at any time. The more types you enable, the more detailed the generated reports will be.

☒ Users	☒ Devices ⚠	☒ Event Logs ⚠
☒ Audit Logs ⚠	☒ MFA Factors ⚠	☒ Groups
☒ Applications	☒ Groups to Users	☒ Applications to Users
☒ Applications to Groups	☒ Named Locations	☒ Direct Reports
☒ Directory Roles	☒ Service Principal	☒ Risky User Events ⚠
☒ Authenticators to Users ⚠	☒ Conditional Access Policy	☒ Provisioning Events ⚠
☒ Device Audit Events ⚠	☒ Mailbox Settings ⚠	☒ Message Rules ⚠
☒ Risky Users ⚠	☒ Registered Devices	

Requires Microsoft Entra ID (formerly Azure AD) Premium P2 subscription

Cancel Save

Where can I see a step by step configuration guide? ^

Refer to [this documentation article](#) for a step by step guidance.

Are Directory ID and Tenant ID the same thing? v

Where do I get my Application ID? v

How do I get my Application Secret Value? v

© 2024 Identity Intelligence

Privacy Policy Terms of Use Documentation SOC2 Report

This environment reloads hourly

Okta Identity Engine



Okta

General Settings

The Okta integration uses an [OAuth2 application in the Okta app catalog](#)

The API is used to get directory information & syncs, but Event Streaming should be used for all log collection

Identity Intelligence

Search

Andy Winiarski
genie

Integrations > Add Integration > Okta

New Okta Integration

General Settings Event Streaming Advanced Settings

Name

Issuer

Client ID

Client Secret

To ensure security, always use the least privileged integration

Cancel Connect

Where can I see a step by step configuration guide?

How do I create an OAuth2 integration?

What are the Okta Event Hooks?

© 2024 Identity Intelligence

This environment reloads hourly

[Privacy Policy](#) [Terms of Use](#) [Documentation](#) [SOC2 Report](#)

Okta

Event Streaming

Okta logs can be streamed to AWS Event Bridge

CII has its own Event Bridge, that Cisco pays for, so the customer does not have to (unlike Azure)

With Event Bridge, it really is more real-time than Azure Event Hub is. CII will get the logs in near-real-time & process

Identity Intelligence

Search

loxx@securityde... security-demo-int

Integrations > Edit Settings

Edit Okta Settings

General Settings **Event Streaming** Advanced Settings

☒ Use Logs Streaming

If you need help configuring Log Streaming, refer to [this documentation article](#).
Use the following values in your Okta instance:

AWS Event Source Name
4e384 [REDACTED]

AWS Account ID
22754 [REDACTED]

AWS Region
US East (Ohio)

☒ I have configured Log Streaming in Okta with the above data

Cancel Save

Where can I see a step by step configuration guide? ^

Refer to [this documentation article](#) for a step by step guidance.

How do I create an Okta API Token? v

Which API Key should I use? v

What are the Okta Event Hooks? v

© 2024 Identity Intelligence

This environment reloads hourly

[Privacy Policy](#) [Terms of Use](#) [Documentation](#) [SOC2 Report](#)

Okta

Advanced Settings

This is where you can tune which information CII should pull when performing sync's with Okta.

Some of the data types require the service account to be assigned Org Admin permissions.

Some of the data types are not available from Okta IdP but require customer to upgrade to Okta Identity Engine (OIE)

CII leverages the information tool-tip to call those out.

Identity Intelligence

Search

loxx@securityde... security-demo-int

Integrations > Edit Settings

Edit Okta Settings

General Settings Event Streaming **Advanced Settings**

Data Types

Check all of the data types you want this integration instance to get. You can update this at any time. The more types you enable, the more detailed the generated reports will be.

☒ Users	☒ Event Logs	☒ Identity Providers
☒ MFA Factors	☒ Groups	☒ Applications
☒ Groups to Users	☒ Applications to Users	☒ Applications to Groups
☒ Policies	☒ API Tokens	☒ Devices ⚠
☒ Policy Rules ⚠	☒ Authenticators ⚠	☒ Authenticators to Users ⚠
☒ User Schema ⚠	Requires Okta Identity Engine	

Requires Org Admin permissions

Cancel Save

Where can I see a step by step configuration guide? ^

Refer to [this documentation article](#) for a step by step guidance.

How do I create an Okta API Token? v

Which API Key should I use? v

What are the Okta Event Hooks? v

© 2024 Identity Intelligence

Privacy Policy Terms of Use Documentation SOC2 Report

This environment reloads hourly

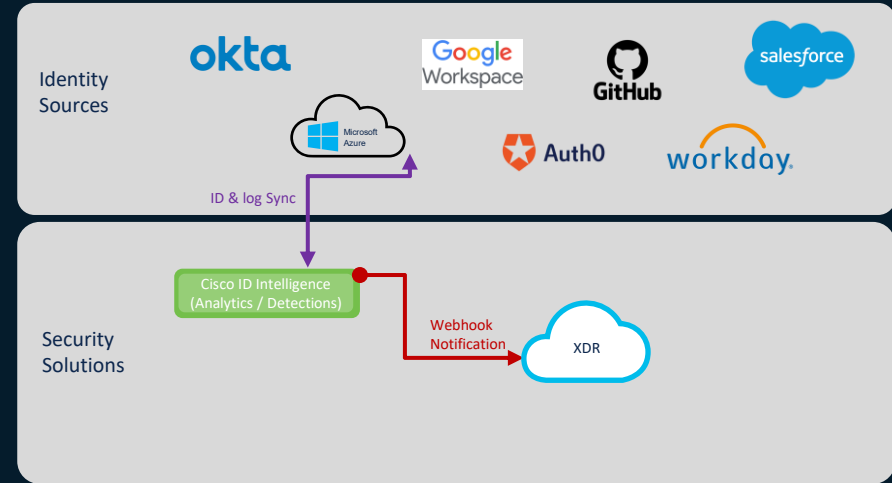
Cisco XDR
Splunk SOAR
etc.

Trick of the Trade



Webhooks

- A callback function that uses HTTP/S between two APIs based on events
 - Send small amounts of data, reactively after a check-fails
 - An example is CII sending a notice to Splunk SOAR or XDR of a check that failed
 - The automation playbook/workflow will extract the appropriate data and then proceed through the rest of the flow



Webhooks w/ Cisco XDR



Webhook URL

XDR listener has specific requirements

- API Key must be in the URL
- 2x Specific headers

Authentication

- CII webhooks require authentication
- But we can lie to it, as long as the key is in the URL
- Here, we lied to it w/ Foo & Fake password

Setup Guide

Published [here at Aaron Woland's blog](#)

General

Display Name* 20 / 64
CII Webhook Listener

Description 92 / 1024

Request Content Type*
application/json

Webhook Details

Webhook ID
foo

Webhook API Key

Copy Refresh

Webhook URL
https://automate.us.security.cisco.com/webhooks/02CWJ

Copy

Integrations > Edit Settings
Edit Webhook Settings

Name
Aaron XDR Listener

Description (optional)
Listener configured in XDR for webhooks

Webhook URL
https://automate.us.security.cisco.com/webhooks/02CWJ

Authorization Type
☐ Basic ☒ API Key ☐ Duo Security Client ☐ OAuth Client Credentials

API key name
foo

API key value

Invocation HTTP Parameters

Parameter	Key name	Key value	
Header	Content-Type	application/json	Remove
Header	Accept	application/json	Remove

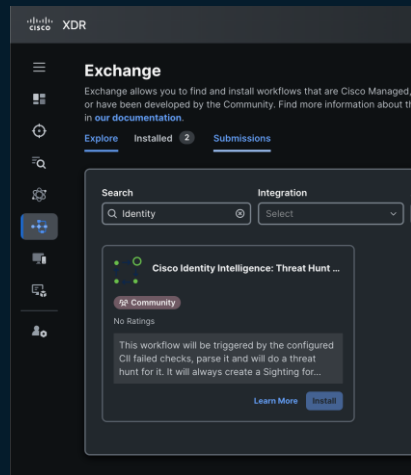
Add parameter

Cancel Save

Webhooks w/ Cisco XDR

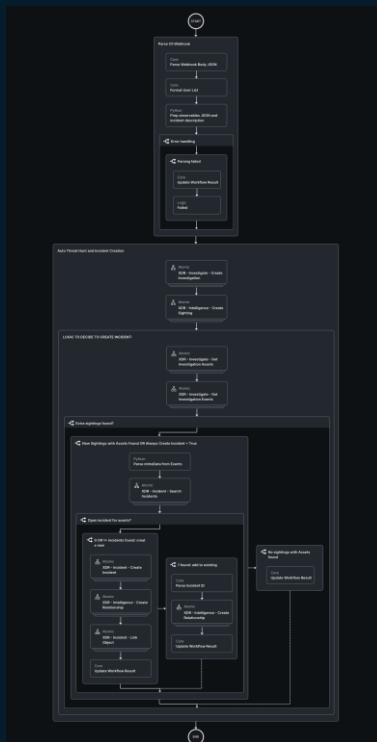
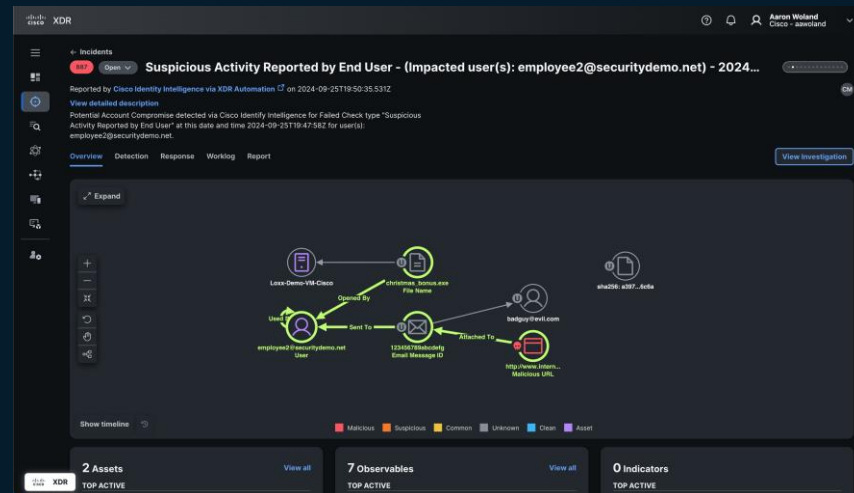
Merges with Incidents

- The CII source events are correlated with the detections from other security products.
- The CII ITDR detection is now part of the attack graph & investigations



Published in Exchange

- A community-maintained XDR workflow.
- Takes the CII Webhook & parses it.
- Will enrich existing incidents, or none exist will create a new incident.



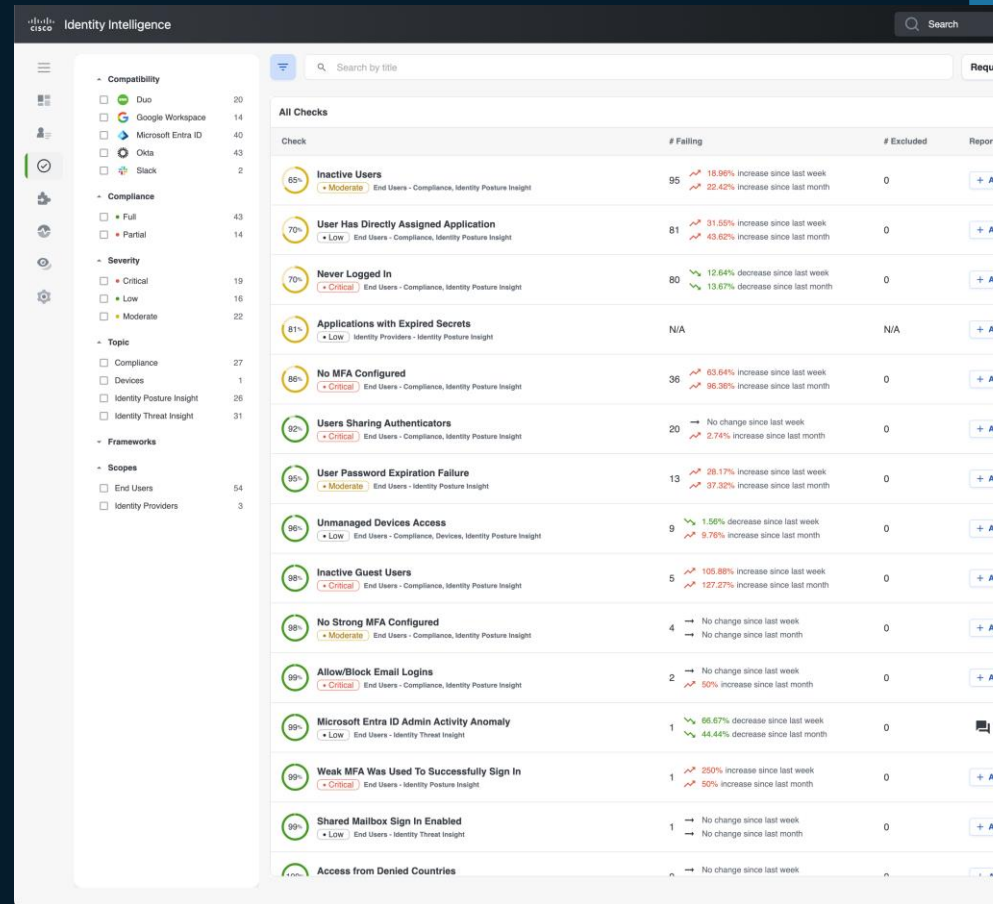


Agenda

- What is Cisco Identity Intelligence
- Integrations
- All about Checks
- Remediations
- Other Technical Nuggets
- Let's talk about APIs
- Call to Action

What are Checks?

- Analytics, detections, rules... like “signatures” in an IDS
- When the collected data matches a check... That check is recorded as failed.



The screenshot displays the Cisco Identity Intelligence interface. On the left, a sidebar contains navigation menus for Compatibility, Compliance, Severity, Topic, Frameworks, and Scopes. The main panel, titled 'All Checks', features a search bar and a table of security checks. Each row in the table includes a check icon, a title, a severity level, a count of failing items, a percentage change since the last week, a count of excluded items, and a percentage change since the last month. The checks listed include Inactive Users, User Has Directly Assigned Application, Never Logged In, Applications with Expired Secrets, No MFA Configured, Users Sharing Authenticators, User Password Expiration Failure, Unmanaged Devices Access, Inactive Guest Users, No Strong MFA Configured, Allow/Block Email Logins, Microsoft Entra ID Admin Activity Anomaly, Weak MFA Was Used To Successfully Sign In, Shared Mailbox Sign In Enabled, and Access from Denied Countries.

Check	# Failing	# Excluded
Inactive Users Moderate End Users - Compliance, Identity Posture Insight	95 18.96% increase since last week 22.42% increase since last month	0
User Has Directly Assigned Application Low End Users - Compliance, Identity Posture Insight	81 31.55% increase since last week 43.62% increase since last month	0
Never Logged In Critical End Users - Compliance, Identity Posture Insight	80 12.64% decrease since last week 13.67% decrease since last month	0
Applications with Expired Secrets Low Identity Providers - Identity Posture Insight	N/A	N/A
No MFA Configured Critical End Users - Compliance, Identity Posture Insight	36 63.64% increase since last week 96.36% increase since last month	0
Users Sharing Authenticators Critical End Users - Compliance, Identity Posture Insight	20 No change since last week 2.74% increase since last month	0
User Password Expiration Failure Moderate End Users - Identity Posture Insight	13 28.17% increase since last week 37.32% increase since last month	0
Unmanaged Devices Access Low End Users - Compliance, Devices, Identity Posture Insight	9 1.56% decrease since last week 9.76% increase since last month	0
Inactive Guest Users Critical End Users - Compliance, Identity Posture Insight	5 105.88% increase since last week 127.27% increase since last month	0
No Strong MFA Configured Moderate End Users - Compliance, Identity Posture Insight	4 No change since last week No change since last month	0
Allow/Block Email Logins Critical End Users - Compliance, Identity Posture Insight	2 No change since last week 50% increase since last month	0
Microsoft Entra ID Admin Activity Anomaly Low End Users - Identity Threat Insight	1 66.67% decrease since last week 44.44% decrease since last month	0
Weak MFA Was Used To Successfully Sign In Critical End Users - Identity Posture Insight	1 250% increase since last week 50% increase since last month	0
Shared Mailbox Sign In Enabled Low End Users - Identity Threat Insight	1 No change since last week No change since last month	0
Access from Denied Countries	No change since last week	No change since last month

Compatibility

Not all checks are compatible with all providers / sources.

You can filter the list of checks based on the IdP source

Topics

Broken into categories and are very filterable.

A single check may belong to multiple Topics

Frameworks

Checks are classified into their applicable risk frameworks – such as CIS, NIST, MITRE ATT&CK TTPs, etc.

The screenshot displays the Cisco Identity Intelligence dashboard. On the left, there are three filter panels: Compatibility, Topics, and Frameworks. The Compatibility panel lists providers like Duo, Google Workspace, Microsoft Entra ID, Okta, and Slack. The Topics panel lists categories like Compliance, Devices, Identity Posture Insight, and Identity Threat Insight. The Frameworks panel lists risk frameworks like End Users, Identity Providers, and Scopes. The main area shows a table of checks with columns for Check name, # Failing, and a status indicator. A search bar is at the top right. A blue box highlights the Frameworks filter and the corresponding rows in the checks table.

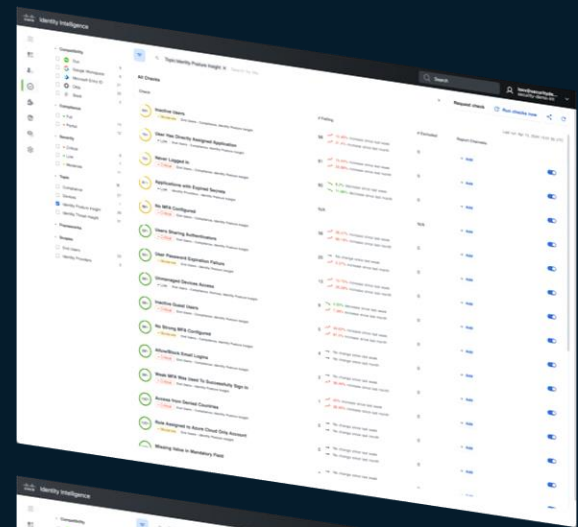
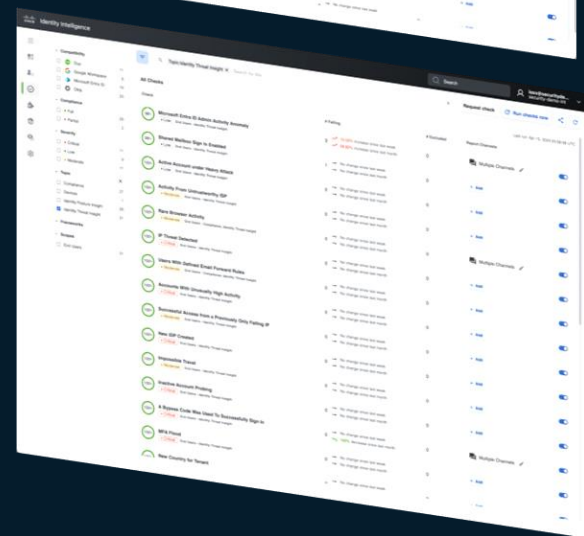
Check	# Failing
Inactive Users	95
User Has Directly Assigned Application	81
Never Logged In	80
Applications with Expired Secrets	N/A
No MFA Configured	36
Users Sharing Authenticators	20
User Password Expiration Failure	13
Unmanaged Devices Access	9
Inactive Guest Users	5
No Strong MFA Configured	4
Allow/Block Email Logins	2

Frameworks

- ☐ ASD Essential 8
- ☐ ASD Level 3
- ☐ CIS 4.3
- ☐ CIS 5.3
- ☐ CIS 5.4
- ☐ CIS 5.5
- ☐ CIS 5.6
- ☐ CIS 6.3
- ☐ CIS 6.4
- ☐ CIS 6.5
- ☐ CMMC AC.2.010
- ☐ CMMC IA.3.083
- ☐ CMMC IA.3.084
- ☐ CMMC SC.3.187
- ☐ Mitre ATT&CK T1078
- ☐ Mitre ATT&CK T1078.004
- ☐ Mitre ATT&CK T1087.004
- ☐ Mitre Mitigation M1032
- ☐ Mitre Mitigation M1036
- ☐ NIST 800-63-3
- ☐ NIST CSF DE.CM-3
- ☐ NIST CSF PR.AC-7
- ☐ NIST CSF PR.IP-11
- ☐ PCI DSS 8.2
- ☐ SOX Section 302.2

Proactive vs. Reactive

- **Posture Checks are Proactive** – examining the authentications and account configurations – to reduce probability and blast radius
- **Threat Checks are Reactive** – examining the behavior of users and their authentications – to detect threats



Checks are Tunable

Check Settings

Depending on the check itself, there are multiple settings that can be adjusted / tuned.

Custom Detection Settings

This one only customizes for exclusion of known-good IP's.

List Settings

In this case, we are defining which events from EntraID are not noteworthy enough to run against the check.

Default was: Ignore Medium & Below

The screenshot shows the Cisco Identity Intelligence interface for the 'Sign in Threat Detected' check. The main page displays details about the check, including its purpose (detecting suspicious sign-ins), severity (Moderate), and recommended actions. Three callout boxes highlight specific settings:

- Custom Detection Settings:** A modal window showing the 'Exclude known good ips' toggle (currently off) and buttons for 'Restore default', 'Save changes', and 'Test'.
- Check Settings:** A panel on the right showing 'Custom Detection Settings' (with an 'Edit' button), 'Notification Settings' (with a 'Customize messages' button), and a list of notification recipients (Aaron XDR Listener, SecurityDemoNet-Ort-Messages, Securitydemo Slack) with 'Test' buttons.
- List Settings:** A modal window showing the 'Ignore list' with buttons for 'Cancel', 'Restore default', '+ Add', and 'Save'. The list contains 5 items: hidden, low, medium, none, and unknownFutureValue. A 'Delete item' button is visible next to the 'low' item.

Outbound Notifications

Notifications

Notifications are configured per check.

Checks are run periodically, matching the data in the CI datastore to the requirements set in the check.

When there is matching criteria, that means a user, device or setting has “failed” that check, and all selected notification channels will be used.

Notifications Targets:

Notification Targets

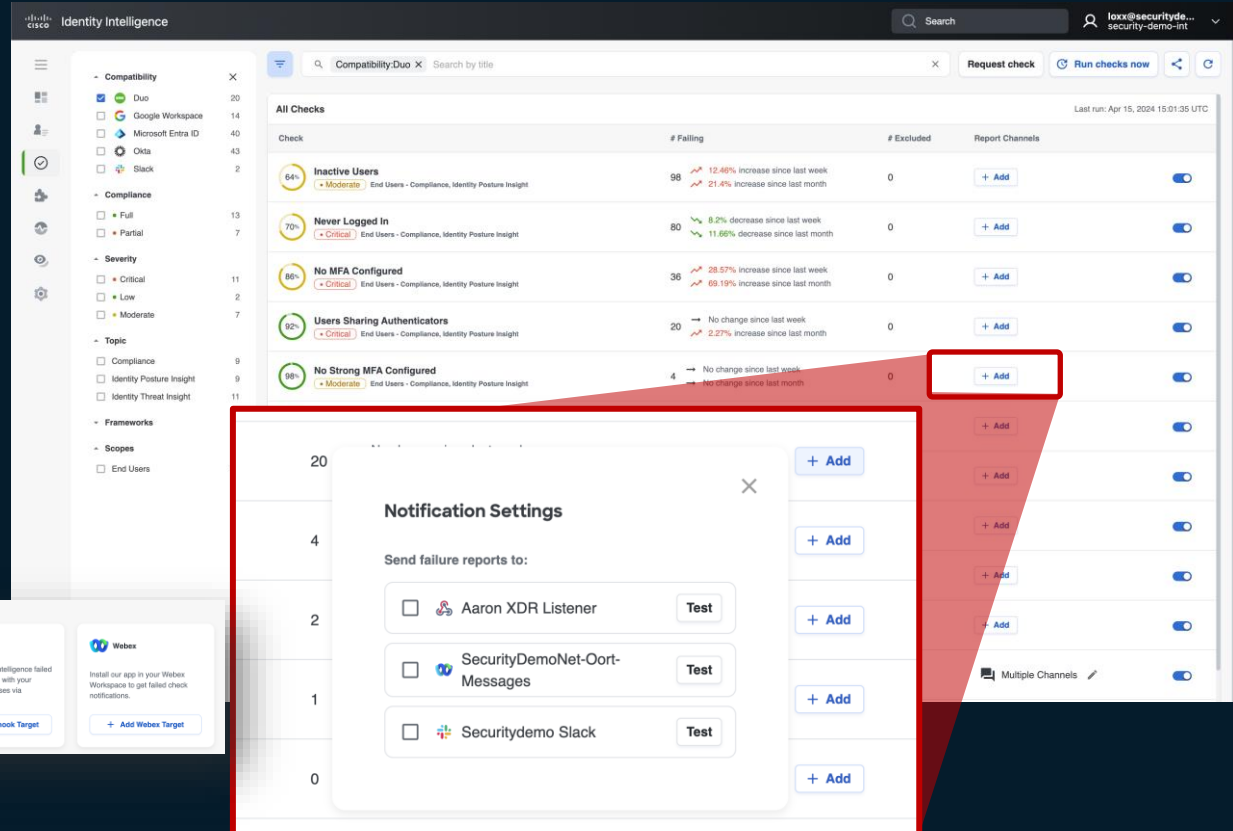

Email address to be used for Identity Intelligence notifications. Adding a different address as CC is supported.
[+ Add Email Target](#)


Install our bot in your Microsoft Teams to get all the latest updates directly or in any public channel you choose.
[+ Add MS Teams Target](#)


Install our app in your Slack Workspace to get all the latest updates directly or in any public channel you choose.
[+ Add Slack Target](#)


Connect Identity Intelligence failed check notifications with your automated processes via webhooks.
[+ Add Webhook Target](#)


Install our app in your Webex Workspace to get failed check notifications.
[+ Add Webex Target](#)



The screenshot displays the Cisco Identity Intelligence interface. On the left, a sidebar shows filters for Compatibility, Compliance, Severity, Topic, Frameworks, and Scopes. The main panel shows a table of checks for 'Compatibility.Duo'. A red box highlights the 'Add' button for the 'No Strong MFA Configured' check. A modal window titled 'Notification Settings' is open, showing a list of notification targets: Aaron XDR Listener, SecurityDemoNet-Oort-Messages, and Securitydemo Slack. Each target has a 'Test' button. The modal also includes a 'Send failure reports to:' section and a 'Multiple Channels' option.

Check	# Failing	# Excluded	Report Channels
Inactive Users	98	0	+ Add
Never Logged In	80	0	+ Add
No MFA Configured	36	0	+ Add
Users Sharing Authenticators	20	0	+ Add
No Strong MFA Configured	4	0	+ Add

Direct User / Manager Notifications

Checks > No MFA Configured
No MFA Configured Critical

Details

Detects users with no Multi-Factor Authentication (MFA) enabled.

MFA requires users to provide something you know, like a password or PIN, or something you have, like an out-of-band device or a one-time password provider. All users should be using MFA to gain access to the system.

Users will not fail this check if they fall within the grace period of 14 days.

You can add known domains to either ignore or include list.

Learn More About the Risk

How Multi Factor Authentication Can Save You

Check Settings

Custom Detection Settings Edit

Grace period for new accounts (days): 14

Notification Settings Customize messages

Send failure reports to:

- ☐ Aaron XDR Listener Test
- ☐ SecurityDemoNet-Oort-Messages Test
- ☐ Securitydemo Slack Test

Send direct messages on failure:

Who should be messaged: **User**

Message channels: **Email**

List Settings Edit

Ignore list

Your don't have any items in your ignore list

49 failing users

User: **secops2@loxx.tv**

Diagram: This way, even if your password was stolen, they don't have

Security Education

CII partners with Wizer (<https://www.wizer-training.com/>) and their very cool security education videos to help educate the end-user on what they did wrong & why it matters.

Educate the End-User

Notifications may be customized and sent to the end user via email or IM.

Chat Ops

- Many Cisco customers do all their workflows through the IM applications like Webex and Slack.
- Provides not only notifications, but also responses such as:
 - Exclude from Check
 - Mark as Interesting
 - Mark as Normal Behavior

The screenshot displays a Slack chat window with a dark theme. On the left, a sidebar shows a search bar and a list of channels, including '#ortb-integration'. The main chat area shows a message from 'Ortb Bot Integration' with a Slack logo. The message content is a Microsoft Entra ID Admin Activity Anomaly alert. The alert includes a severity level of 'Low', a timestamp of '12 Apr 2024 15:01 GMT', and references to 'Identity Threat Insight | CIS 5.4 NIST CSF PR.AC-4' and 'NIST CSF DE.CM-3 Mitre ATT&CK T1098.003'. It describes a detection of new administrative actions performed by an account on multiple targets simultaneously. The alert also mentions that Identity Intelligence detects recent administrative actions within the past 90 days, alerting on those performed by an account on 10 or more targets within a 10-minute period. It further states that adversaries may create/modify an account to maintain access to victim systems or to modify the configuration settings to evade defenses and/or escalate privileges. Below the alert text, there are three buttons: 'Exclude from check', 'Interesting', and 'Normal behavior'. The 'Interesting' button is highlighted. Below these buttons, there is a list of users: 'azita@securitydemo.net' and 'prakasp3@cisco.com'. The message also includes an 'Integration ID: SecDemo-EntraID' and a description of the user's actions: 'user performed 59 ApplicationManagement actions on 59 distinct targets over 10 minutes'. Below this, there is another set of buttons: 'Exclude from check', 'Interesting', and 'Normal behavior', with 'Interesting' again highlighted. Further down, there is a section titled 'Recommended Actions' with a note about verifying the account and a 'Go to report' button. On the right side of the chat window, there is a sidebar with a search bar and a list of channels, including '#ortb-integration'. The main chat area on the right shows a message from 'Ortb Bot Integration' with a Slack logo. The message content is a Microsoft Entra ID Admin Activity Anomaly alert. The alert includes a severity level of 'Low', a timestamp of '12 Apr 2024 15:01 GMT', and references to 'Identity Threat Insight | CIS 5.4 NIST CSF PR.AC-4' and 'NIST CSF DE.CM-3 Mitre ATT&CK T1098.003'. It describes a detection of new administrative actions performed by an account on multiple targets simultaneously. The alert also mentions that Identity Intelligence detects recent administrative actions within the past 90 days, alerting on those performed by an account on 10 or more targets within a 10-minute period. It further states that adversaries may create/modify an account to maintain access to victim systems or to modify the configuration settings to evade defenses and/or escalate privileges. Below the alert text, there are three buttons: 'Exclude from check', 'Interesting', and 'Normal behavior'. The 'Interesting' button is highlighted. Below these buttons, there is a list of users: 'azita@securitydemo.net' and 'prakasp3@cisco.com'. The message also includes an 'Integration ID: SecDemo-EntraID' and a description of the user's actions: 'user performed 59 ApplicationManagement actions on 59 distinct targets over 10 minutes'. Below this, there is another set of buttons: 'Exclude from check', 'Interesting', and 'Normal behavior', with 'Interesting' again highlighted. Further down, there is a section titled 'Recommended Actions' with a note about verifying the account and a 'Go to report' button.



Agenda

- What is Cisco Identity Intelligence
- Integrations
- All about Checks
- Remediations
- Other Technical Nuggets
- Let's talk about APIs
- Call to Action

Taking Action(s)

Remediation is available through CII, but it is up to the customer to determine if direct remediation is right for the organization

- Organizations have invested heavily in their response flows with ticketing systems like ServiceNow, or Automation Tools like XDR and SOAR.
- Those organizations should use webhooks to notify those other systems & respond through a robust workflow.

Remediations are source specific

- Not all sources support the same remediation.
- Reset MFA is applicable to Okta & Duo only (for example)

Remediation Nuggets:

- CII only allows one remediation action at a time.
- The provider must be configured to allow the actions (think “*write*” access)

Context Specific Remediation Menu

- As of Sept 2024 – only shows the remediation actions applicable for that user
- Only actions that are available for the sources that user is found in
- Only active integrations

The screenshot displays the Cisco Duo user management interface. At the top, a search bar shows 'NOT Status:(3 conditions) Aaron'. Below, a table lists two users found:

User	Checks	# IPs	# Logins	Last Seen (UTC)	Last IP Address	Last Location	MFA	Providers	Status
Aaron Woland aawoland	⏸	0	N/A	A Day Ago Apr 23, 2024 15:14:37	N/A	N/A	✓	🔄	Inconsistent
Aaron Woland aawoland@cisco.com	✓	7	23	A Day Ago Apr 23, 2024 15:14:37	N/A	N/A	✓	🔄 ⚙️ 🌐	Active

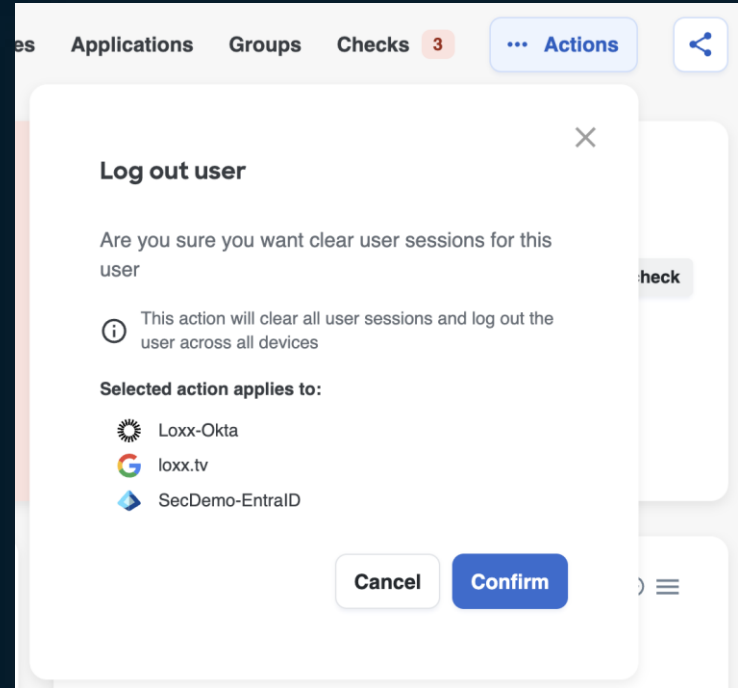
Two detailed views of the 'Actions' menu are shown on the right:

- Inconsistent User (aawoland):** The 'Actions' menu (purple box) includes 'Open ticket', 'Refresh User Data', and 'Link user'.
- Active User (aawoland@cisco.com):** The 'Actions' menu (red box) includes 'Open ticket', 'Reset MFA', 'Log out user', 'Quarantine', 'Send push verification', 'Refresh User Data', and 'Link user'.

Red and purple lines connect the status icons in the table to their respective detailed views.

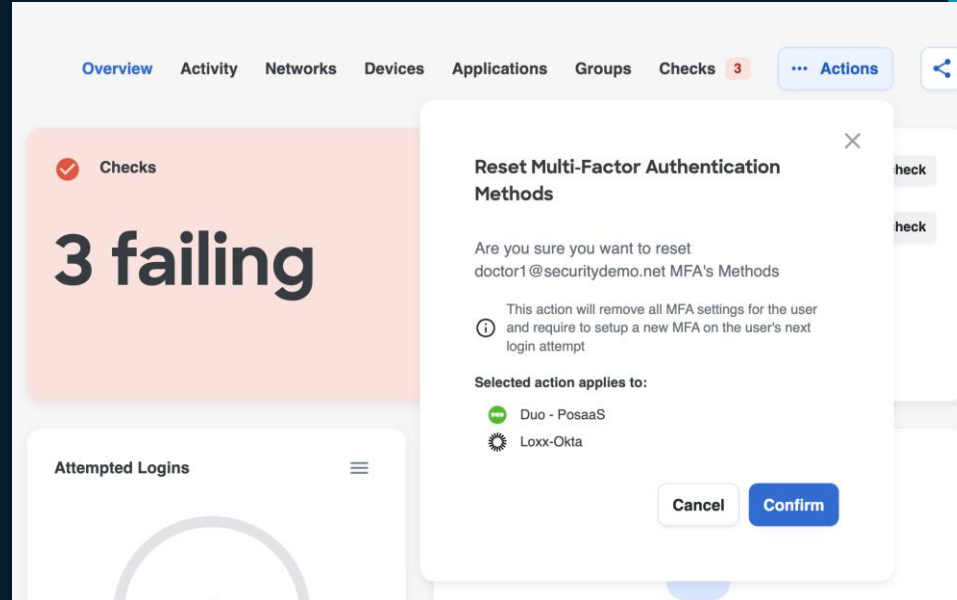
Log Out User

- Clears all user sessions
 - Logs out the user across apps that support action (O365, for example)
- Remember how WebAuth protocols work:
 - IDP signs token, session is issued based on valid token.
 - Session has expiration time
 - Until that time, session is VALID
 - Apps do not check with IDP again during that valid time
 - Sessions can last hours, days, or longer



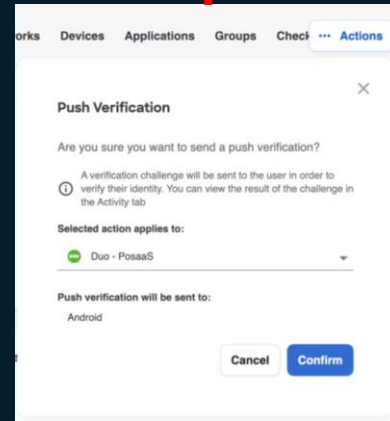
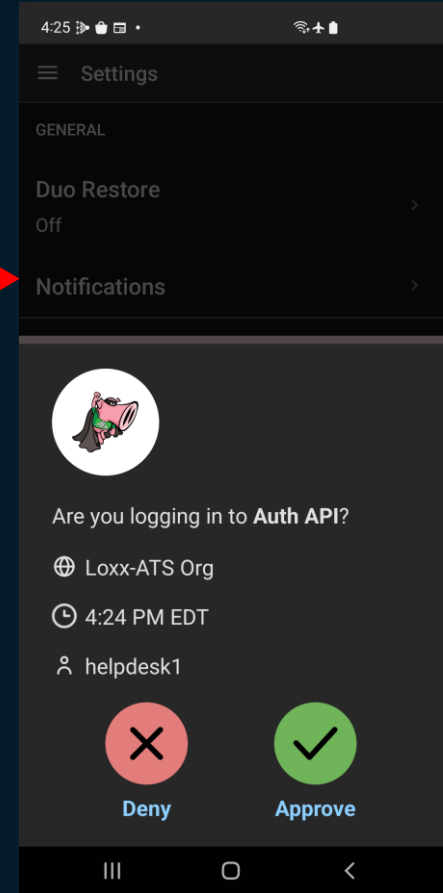
Reset MFA example w/ Duo

- CII queries the Duo Admin API
 - Learns all phones associated to user
 - Learns all hardware tokens for user
- CII Disassociates the user from the all their phones and tokens
 - User is as if they are brand-new
 - Have to setup MFA from scratch



Send Push Notification

- To verify a user's identity
 - Send the user a one-time push notification to confirm they are who they say they are
 - Very helpful for help-desks to verify human calling them is indeed who they say they are
- Select the MFA provider
 - Click Confirm
 - Push notification is sent





Agenda

- What is Cisco Identity Intelligence
- Integrations
- All about Checks
- Remediations
- Other Technical Nuggets
- Let's talk about APIs
- Call to Action

Account Merges

- Accounts from different IDPs are merged when:
 - UPN, email, Employee ID, or Duo Alias match.
- No “or” logic today. Must use one.

This screenshot shows the Duo user management interface for a user named 'employee1'. The 'Username aliases' section contains two entries: 'Username alias 1' with the value '123456789' and 'Username alias 2' with the value 'employee1@securitydemo.net'. The 'Email' field at the bottom is also set to 'employee1@securitydemo.net'. Red boxes highlight the 'Username alias 2' field and the 'Email' field, with red lines connecting them to the corresponding fields in the other two screenshots.

This screenshot shows the Microsoft Azure portal user profile for 'EmployeeOne'. The 'Basic info' section displays the 'User principal name' as 'employee1@securitydemo.net' and the 'Object ID' as '101e3689-1337-4df5-98f8-b5cbd46d1910'. Red boxes highlight the 'User principal name' field and the 'Object ID' field, with red lines connecting them to the corresponding fields in the other two screenshots.

This screenshot shows the Okta user profile for 'Employee One'. The 'Attributes' section displays the 'Username login' as 'employee1@securitydemo.net'. Red boxes highlight the 'Username login' field and the 'Object ID' field from the Microsoft Azure screenshot, with red lines connecting them to the corresponding fields in the other two screenshots.

Linking Accounts

Not a merge, a linkage

For example, a privileged admin creates a service account.

That admin leaves company, HR system deletes the user's account; but the service-account will still exist with full privileges!

Linked Users + Add						
User	Status	User Type	Last Seen (UTC)	Last Location	MFA	Providers
Service Account   serviceaccount@securitydemo.net	• Active	Service Account	16 Days Ago Apr 2, 2024 13:19:55	Cary, NC, US		  
Loxx   loxx@securitydemo.net	• Active	Inconsistent	12 Hours Ago Apr 17, 2024 15:37:33	N/A		   

Suggesting Linkages

Link Suggestions

CII will merge accounts automatically.

When it seems similar accounts that aren't mergeable, it will suggest linking.

Link Suggestions

I call this the "Google photos" feature..

Is this the same user?

- Link
- Reject
- Skip for now

The screenshot displays the Cisco Identity Intelligence (CII) web interface. At the top, the header shows the Cisco logo, the text "Identity Intelligence", a search bar, and the user profile of Aaron Woland. The main content area shows the user profile for "aawoland@cisco.com", which is marked as "Active". Below the profile, there are tabs for Overview, Activity, Networks, Devices, Applications, Groups, Checks, and Actions. A yellow box highlights a notification: "Users aawoland@cisco.com and several others have the same user name. Do you want to link them?". Below this, a dialog box titled "These accounts might belong to the same user" is open. It contains the text: "Review the following users that we identified with the same employee ID or similar usernames. Select users you would like to link with aawoland@cisco.com". Below this, it says: "To add or remove existing linked users from this profile, go to the 'Linked Users' table." The dialog lists two accounts with the same username: "Aaron Woland" (aawoland) and "Aaron Woland" (aawoland@cisco.com). Each account has a radio button next to it, with labels "Link", "Reject", and "Skip for now" below the buttons. At the bottom of the dialog are "Cancel" and "Confirm Linkage" buttons.

Threat Intel Nuggets

- How CII knows about ISP details for checks like “Activity From Untrustworthy ISP” & “Personal VPN Usage”:
- CII is using the ASN of the service provider
- Subscribe to IPInfo feed categories:
 - Hosting
 - Proxy
 - Tor
 - Vpn
 - Relay
 - Service
 - Malicious IP
 - Password Spray

The screenshot displays the Cisco Identity Intelligence (CII) dashboard. The left sidebar shows navigation options like Compatibility, Compliance, Severity, Topic, Frameworks, and Scopes. The main area lists various checks with their status, severity, and trends. Two checks are highlighted with a red box:

- Activity From Untrustworthy ISP**: Status 100%, Severity Moderate, End Users - Identity Threat Insight. Trends: No change since last week, No change since last month.
- IP Threat Detected**: Status 100%, Severity Critical, End Users - Identity Threat Insight. Trends: No change since last week, No change since last month.

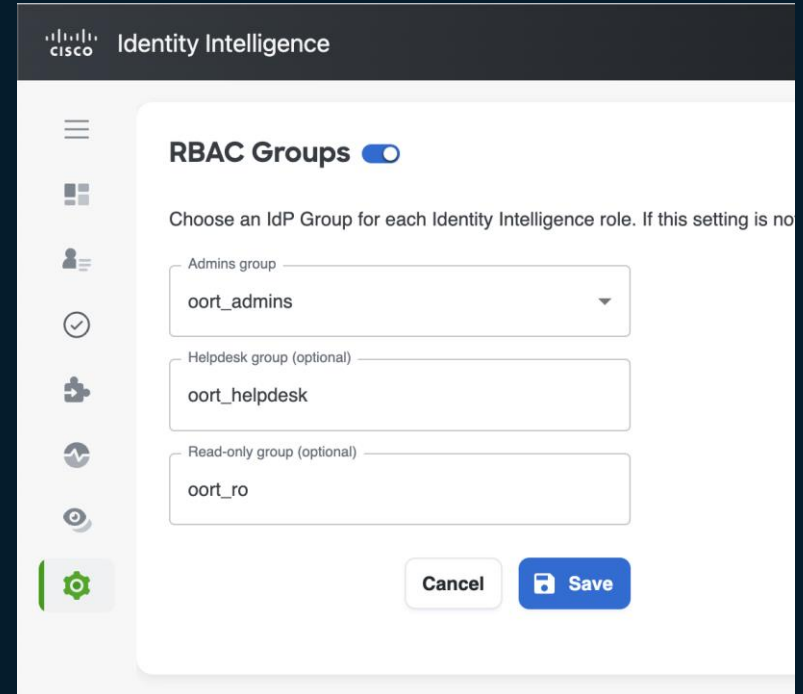
A zoomed-in view of these two checks is shown at the bottom, enclosed in a red box.

Check	# Failing	# Excluded	Report Channels
Sign in Threat Detected	1	0	Multiple Channels
Shared Mailbox Sign in Enabled	1	0	+ Add
Active Account under Heavy Attack	0	0	+ Add
Activity From Untrustworthy ISP	0	0	+ Add
IP Threat Detected	0	0	+ Add
Users With Defined Email Forward R...	0	0	+ Add
Accounts With Unusually High Activity	0	0	+ Add
Successful Access from a Previously...	0	0	+ Add

Check	# Failing	# Excluded	Report Channels
Activity From Untrustworthy ISP	0	0	+ Add
IP Threat Detected	0	0	+ Add

Role Based Access Control

- Three built in Roles:
 - Admins (Full Administrator)
 - Helpdesk
 - Read-only
- Manage roles via groups in the IDP
- No local admin accounts – IDP only



The screenshot shows the 'Identity Intelligence' configuration page for 'RBAC Groups'. The page has a dark header with the Cisco logo and 'Identity Intelligence' text. A left sidebar contains icons for navigation. The main content area is titled 'RBAC Groups' with a toggle switch that is turned on. Below the title, there is a descriptive text: 'Choose an IdP Group for each Identity Intelligence role. If this setting is no'. There are three dropdown menus: 'Admins group' with 'oort_admins' selected, 'Helpdesk group (optional)' with 'oort_helpdesk' selected, and 'Read-only group (optional)' with 'oort_ro' selected. At the bottom right, there are 'Cancel' and 'Save' buttons.

Identity Intelligence

RBAC Groups ☒

Choose an IdP Group for each Identity Intelligence role. If this setting is no

Admins group

Helpdesk group (optional)

Read-only group (optional)

Advanced Search

- Switch to advanced mode
 - Uses Kibana Query Language (KQL)
 - Provides search operators:
 - AND
 - OR
 - NOT
 - _exists_
 - !_exists_
 - Use **CTL + Space** to get list of advanced query attributes
 - Save your adv queries in the UI!

The screenshot shows the Cisco Identity Intelligence Advanced Search interface. The search bar contains the query 'NOT Status (3 conditions) AND ...'. A 'Switch to advanced mode' dialog box is open, explaining that clicking the button switches to advanced mode where custom queries can be input. The main results table displays user information, including names, email addresses, and various attributes like 'Accounting1', 'Accounting2', 'Adam Sonnenfeld', 'Aditya Sankar', 'Ahmadreza Edalat', 'Alex Dipasquale', 'Alex Wight', 'Alex Zaslavsky', and 'Alice Smith'. Each row includes a status indicator (red or green), a count, and a date.



Agenda

- What is Cisco Identity Intelligence
- Integrations
- All about Checks
- Remediations
- Other Technical Nuggets
- Let's talk about APIs
- Call to Action

CII Public API

- <https://docs.oort.io/public-api/apis>
- GraphQL based API
 - Why graphql – don't have to send EVERYTHING in the response..
 - Your request is structured as a query & CII sends only what you ask for.
- GraphQL self-documents its schema
- CII provides Postman collection, downloadable right from documentation

The screenshot shows the 'Oort Knowledge Base' website. The left sidebar contains a navigation menu with links: Home, Glossary, Best Practices, How-to Guides, Oort Insights, Integrations, **Public API** (highlighted), APIs, Troubleshooting & Support, and Release Notes. The main content area displays a list of steps for using the API, including extracting an access token and setting an Authorization header. Below this, there is a section titled 'Using a Postman Collection' which instructs users to import a collection and follow the instructions in the 'overview' tab. A download button for 'Cisco Identity Intelligence Public API.postman_collection.json' (11KB) is provided. At the bottom, there are navigation links for 'Previous Report as a Service (RaaS)' and 'Next APIs', and a footer indicating the page was 'Last updated 14 days ago' and is 'Powered by GitBook'.

docs.oort.io/public-api

Oort Knowledge Base

Home
Glossary
Best Practices
How-to Guides
Oort Insights
Integrations
Public API
APIs
Troubleshooting & Support
Release Notes

2. Extract the **access_token** from the response.
An access token is valid for 10 hours.
3. When invoking the public API requests set an **Authorization** header with the value
`Bearer <value of access_token >`

Using a Postman Collection

Import the attached Postman collection and follow the instructions in the collection **overview** tab.

11KB Cisco Identity Intelligence Public API.postman_collection.json

Previous
Report as a Service (RaaS)

Next
APIs

Powered by GitBook

Last updated 14 days ago

GraphQL Explorer Tools

- Hasura GraphQL Explorer
 - Wraps around the open_source GraphQL UI
 - Exposes an “explorer” that allows you to check-off the fields you want, in order to build your specific query
 - [https://cloud.hasura.io/public/graphql?endpoint=\[INSERT_URL\]](https://cloud.hasura.io/public/graphql?endpoint=[INSERT_URL])


This is an API preview. Create your own API with Hasura Cloud.
Go to Hasura Cloud

GraphQL Endpoint

POST Change Endpoint

Request Headers

ENABLE	KEY	VALUE
☒	content-type	application/json
☒	Authorization	eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCIsImtpc2I6IjUwVWV3NWdnMlVncENSY0k4d2M3aCJ9.ejYpc3
	Enter Key	Enter Value

Explorer

×

GraphiQL

▶

Prettify

History

Explorer

Share

Code Exporter

Merge

Copy

◀ Docs

query MyQuery

getEndUser

getEndUserState

getEndUsersByIp

getIntegrationsStatus

getTotalCheckFailingCounts

listAdminLogins

listEndUsers

input:

orderBy:

pageSize:

pageToken:

items

company

department

devices

deviceType

deviceId

displayName

lastSeen

os

provider

display

displayName

emails

employeeIds

failingChecks

groupNames

firstCreatedDate

hasMoreGroups

id

lastActive

lastSignIn {

ipAddress

location {

city

country

```

1 query MyQuery {
2   listEndUsers(input: {}) {
3     items {
4       company
5       department
6       devices {
7         deviceType
8         deviceId
9         displayName
10        lastSeen
11        os
12        provider
13      }
14      displayName
15      emails
16      employeeIds
17      failingChecks
18      groupNames
19      firstCreatedDate
20      hasMoreGroups
21      id
22      lastActive
23      lastSignIn {
24        ipAddress
25        location {
26          city
27          country

```

```

{
  "data": {
    "listEndUsers": {
      "items": [
        {
          "company": null,
          "department": null,
          "devices": [],
          "displayName": "aaron@woland.com",
          "emails": null,
          "employeeIds": null,
          "failingChecks": [],
          "groupNames": [],
          "firstCreatedDate": null,
          "hasMoreGroups": false,
          "id": "4e384171-e293-4c17-a2da-ba50dc445f54_aaron@woland.com",
          "lastActive": null,
          "lastSignIn": null,
          "linkedEndUserLogins": null,
          "login": "aaron@woland.com",
          "managerLogin": null,
          "mfaEnabled": false,
          "phoneNumbers": [],
          "providers": [
            "SLACK"
          ],
          "isActive": "INACTIVE"
        }
      ]
    }
  }
}

```



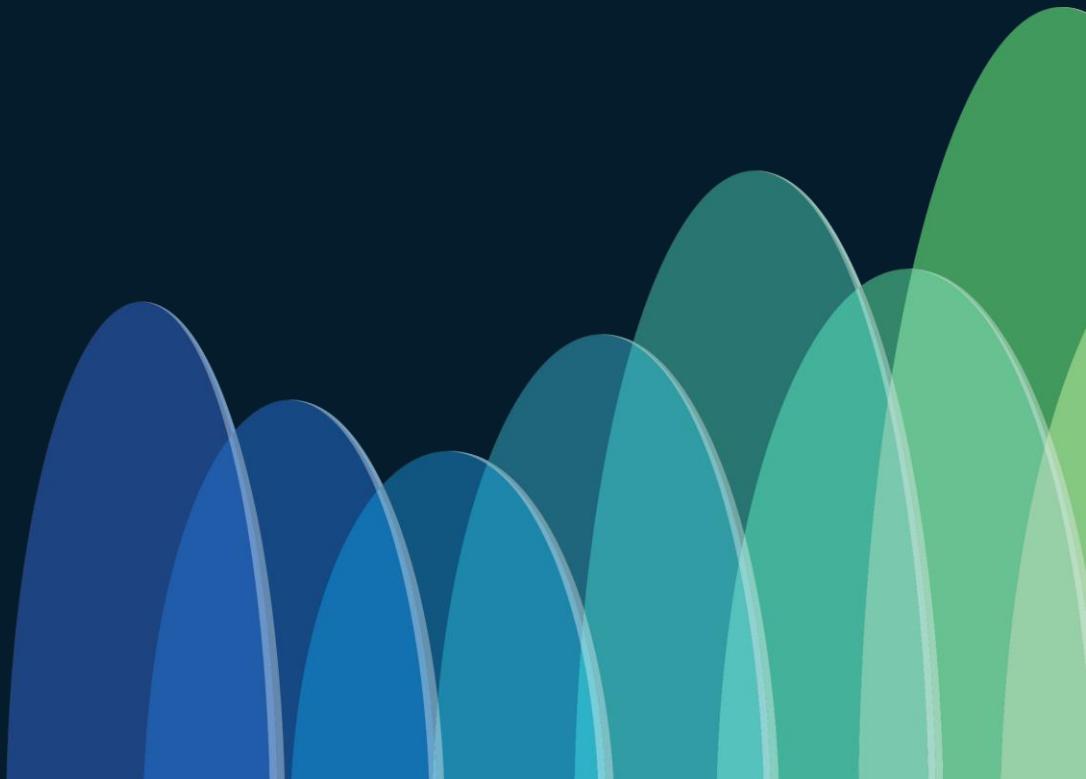
Agenda

- What is Cisco Identity Intelligence
- Integrations
- All about Checks
- Remediations
- Other Technical Nuggets
- Let's talk about APIs
- Call to Action

Call to Action

- Login to the [CII demo tenant](#) (“Genie”) & get a feel for Identity Intelligence
 - Sign in with a social login option (Gmail, LinkedIn, etc)
- Provision your own CII tenant from Duo
 - Included with Duo Advantage or above
 - Free trial of Premier Edition
- Free [Identity Security Assessment](#)

Q & A



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC