cisco The bridge to possible

Identity Intelligence Demystified

Cisco's acquisition of Oort

Aaron T Woland, CCIE #20113
Distinguished Security Engineer
loxx@cisco.com | 𝕏 @aaronwoland | in aaronwoland
BRKSEC-2162

Cisco Webex App

Questions?

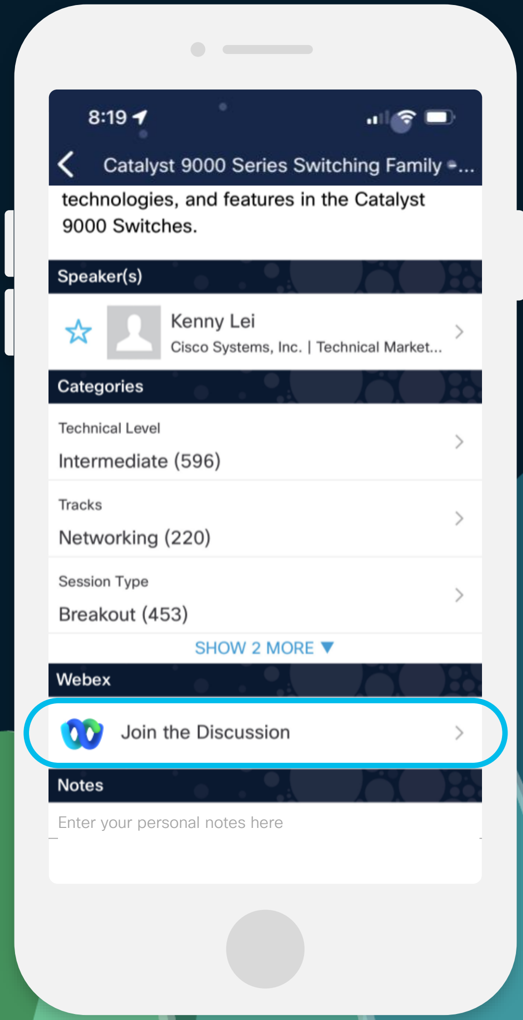
Use Cisco Webex App to chat
with the speaker after the session

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 June 7, 2024.

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



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

$ 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

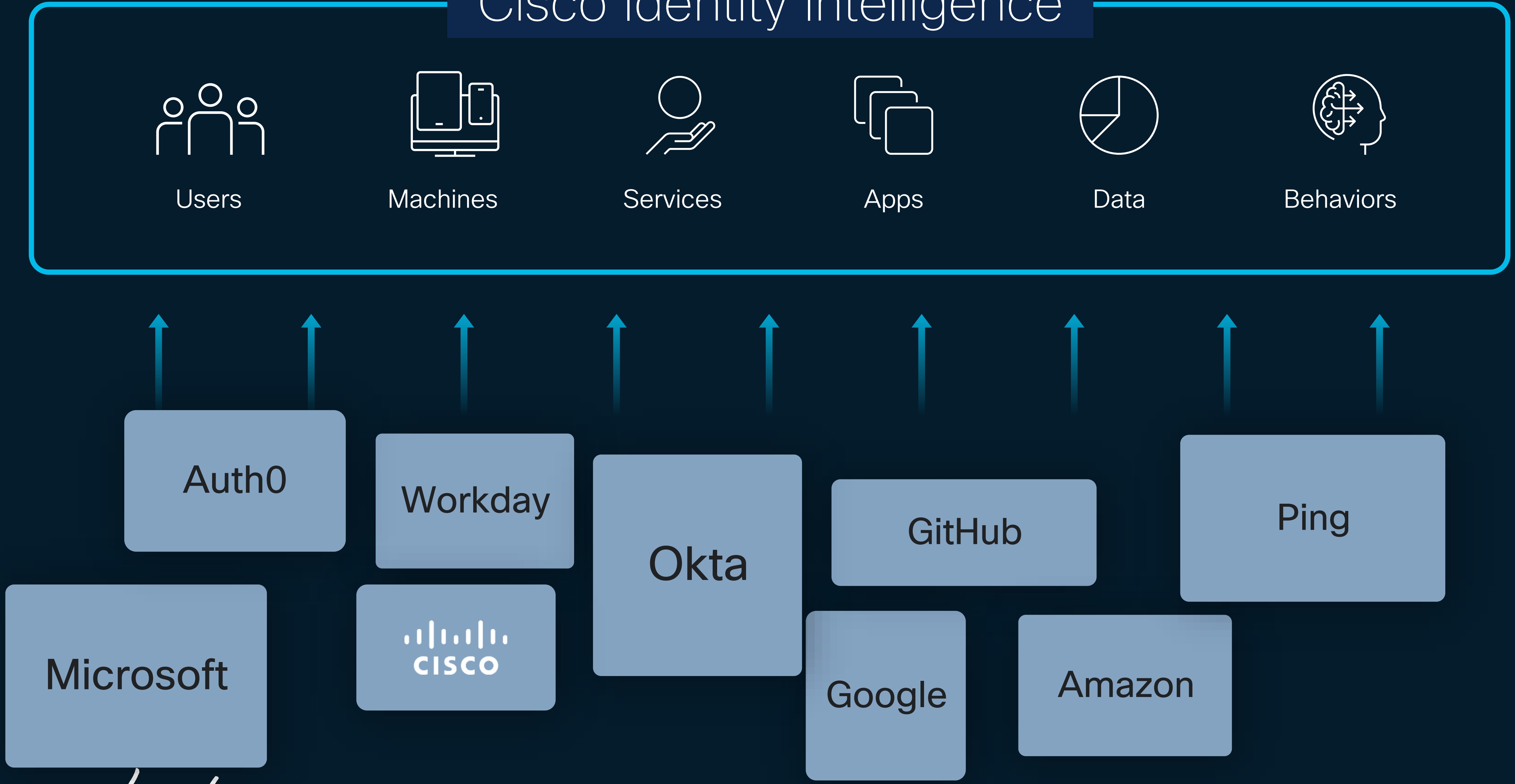
Fun fact 2: Oldest works for Cisco now! Youngest is 2!

Fun fact 3: Working through his Cyber Security Master’s Degree from SANS Institute (~07/24)

Agenda

- What is Cisco Identity Intelligence
- Integrations
- All about Checks
- Session Hijacking Example
- 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

Ping

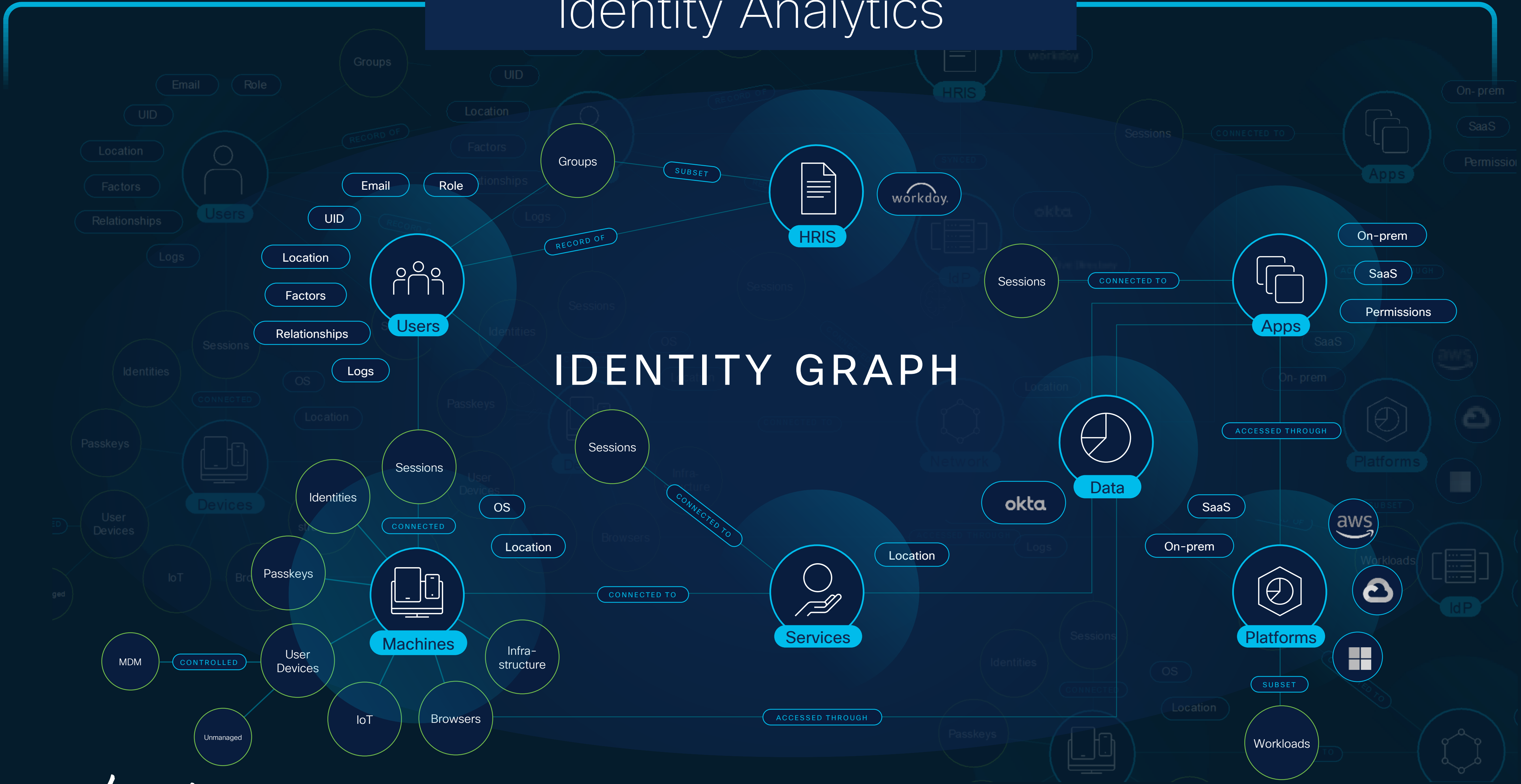
Microsoft

cisco

Google

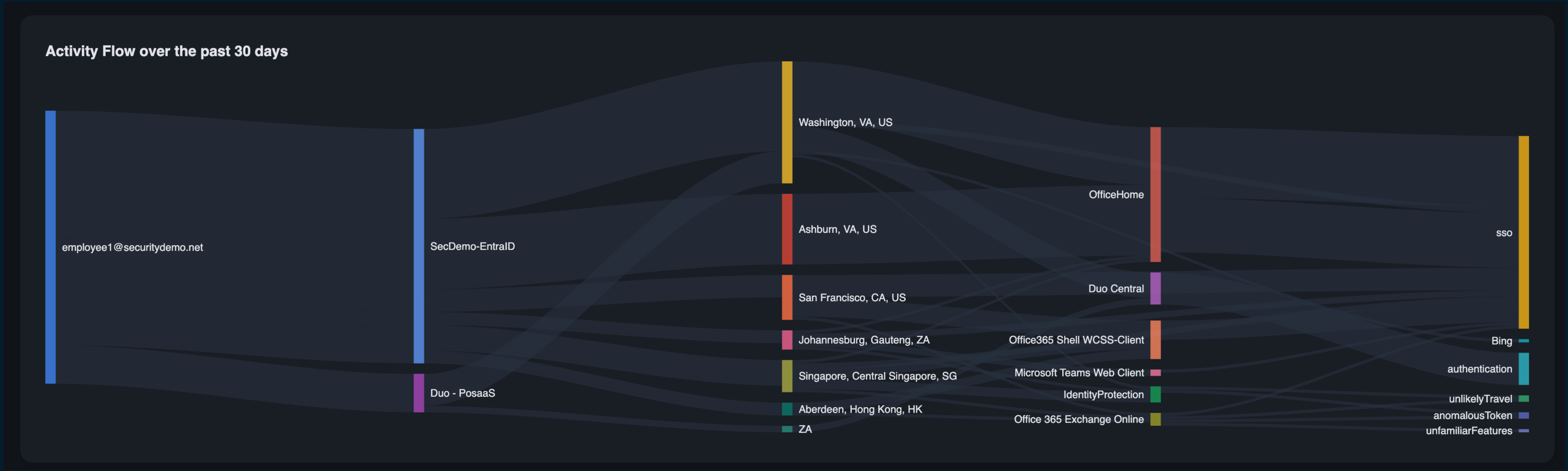
Amazon

Identity Analytics

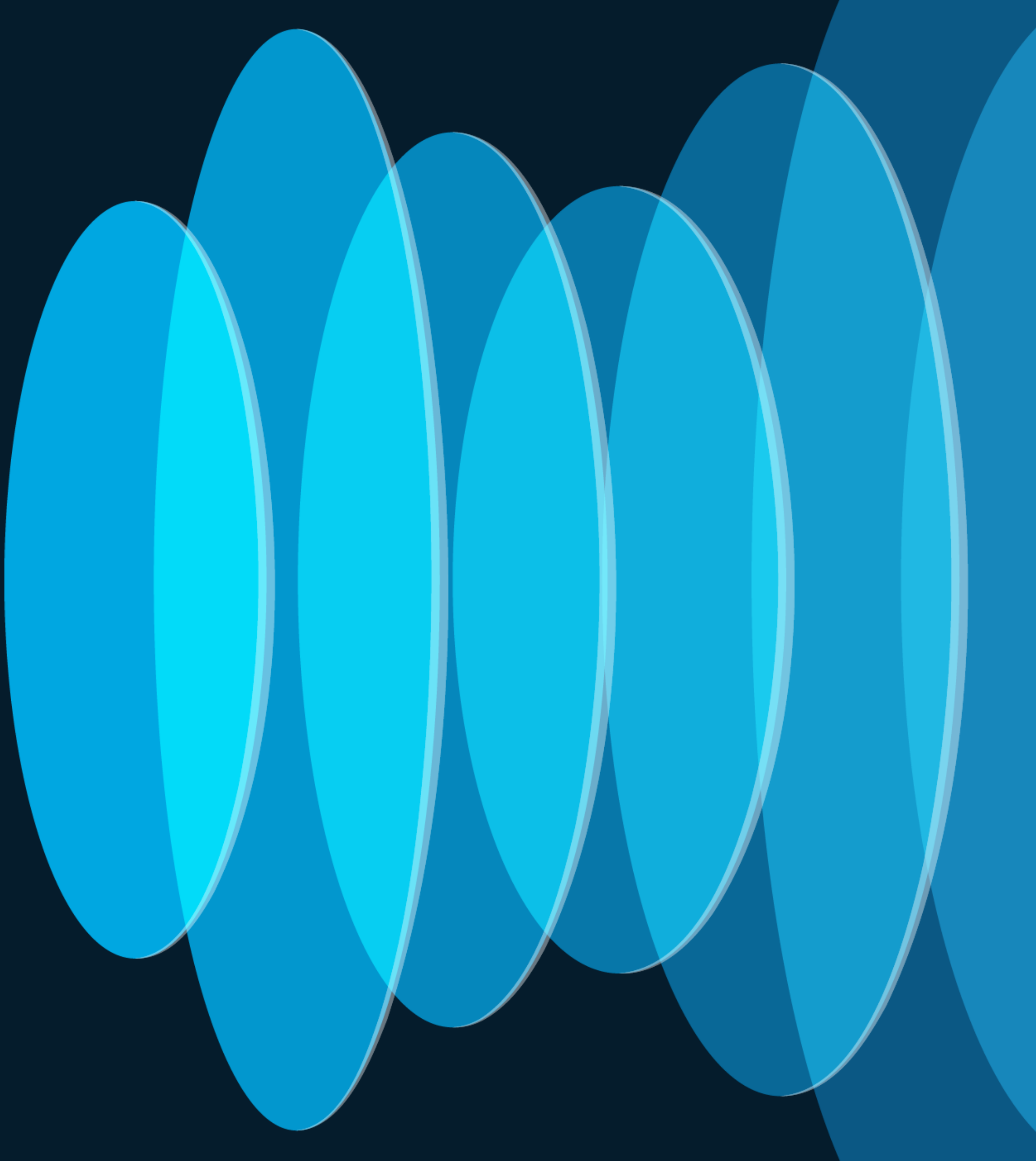


Real life example of detection

Identity graph - Threat analysis based on probed account


Activity Flow over the past 30 days

Now that you heard the marketing, let’s talk about how customers use CII & why!



Wait... Why not just use the IDP?

- Okta, Duo, Microsoft – they all claim to provide ID security!
  - But they can only detect what they see!
  - Most organizations have multiple IDPs, each one is separate
- 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 alerts from Entra, and I cannot believe how bad Entra is at using their own alerts"*
> *- Fortune 100 Manufacturing Co*

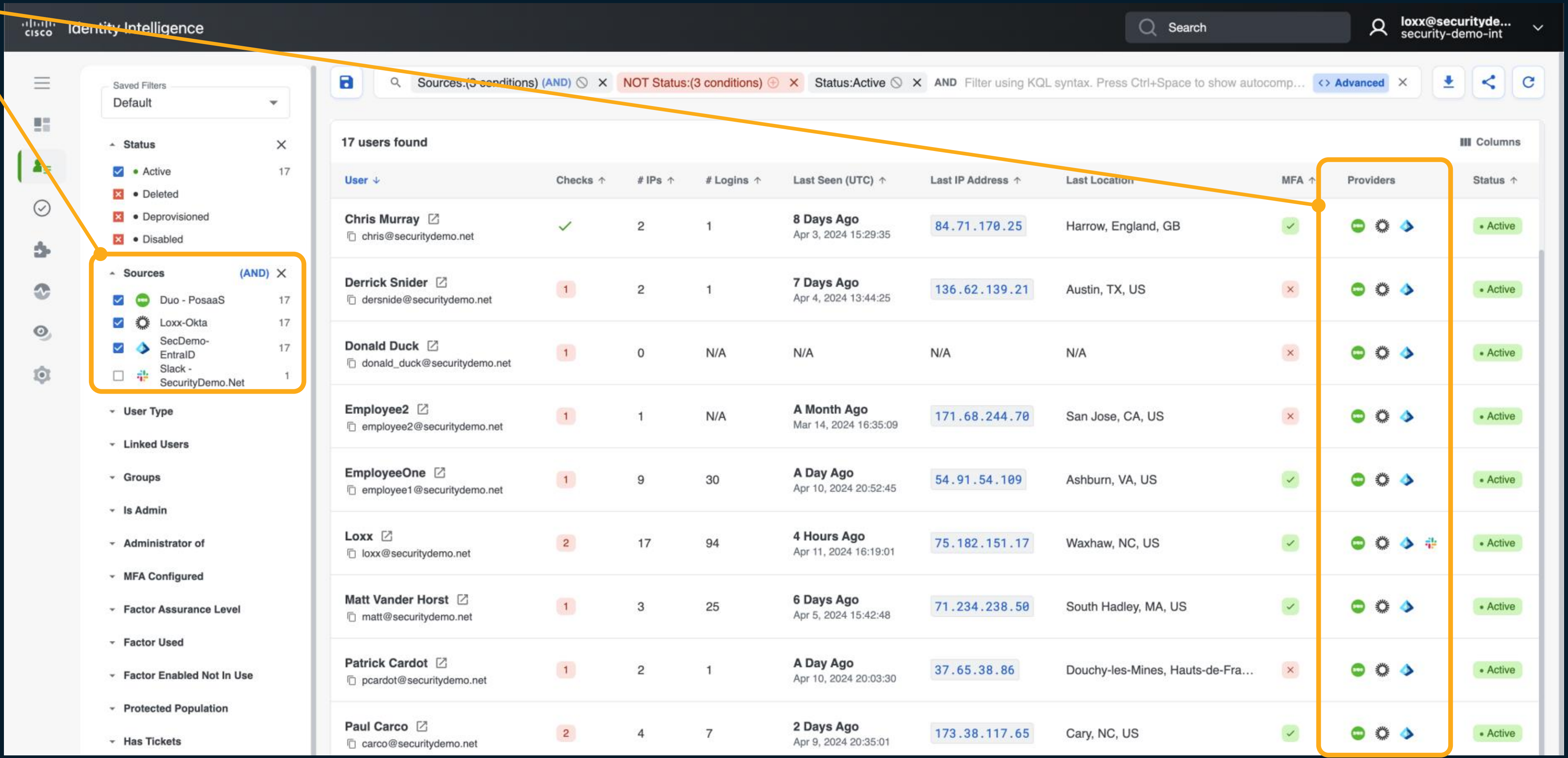
Demo: User 360 & Integration Overview

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.



Saved Filters: Default

Status
- ☑ • Active 17
- ☒ • Deleted
- ☒ • Deprovisioned
- ☒ • Disabled

Sources (AND)
- ☑ Duo - PosaaS 17
- ☑ Loxx-Okta 17
- ☑ SecDemo-EntraID 17
- □ Slack - SecurityDemo.Net 1

User Type · Linked Users · Groups · Is Admin · Administrator of · MFA Configured · Factor Assurance Level · Factor Used · Factor Enabled Not In Use · Protected Population · Has Tickets

Sources:(3 conditions) (AND) · NOT Status:(3 conditions) · Status:Active · AND Filter using KQL syntax. Press Ctrl+Space to show autocomp… · Advanced

17 users found

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	84.71.170.25	Harrow, England, GB	✓	● ✹ ◆	• 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	✕	● ✹ ◆	• Active
Donald Duck donald_duck@securitydemo.net	1	0	N/A	N/A	N/A	N/A	✕	● ✹ ◆	• 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	✕	● ✹ ◆	• Active
EmployeeOne employee1@securitydemo.net	1	9	30	A Day Ago Apr 10, 2024 20:52:45	54.91.54.109	Ashburn, VA, US	✓	● ✹ ◆	• Active
Loxx loxx@securitydemo.net	2	17	94	4 Hours Ago Apr 11, 2024 16:19:01	75.182.151.17	Waxhaw, NC, US	✓	● ✹ ◆ ✱	• 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	✓	● ✹ ◆	• 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…	✕	● ✹ ◆	• 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	✓	● ✹ ◆	• Active

Users

User 360 View

The user details is known as the "user 360 view"

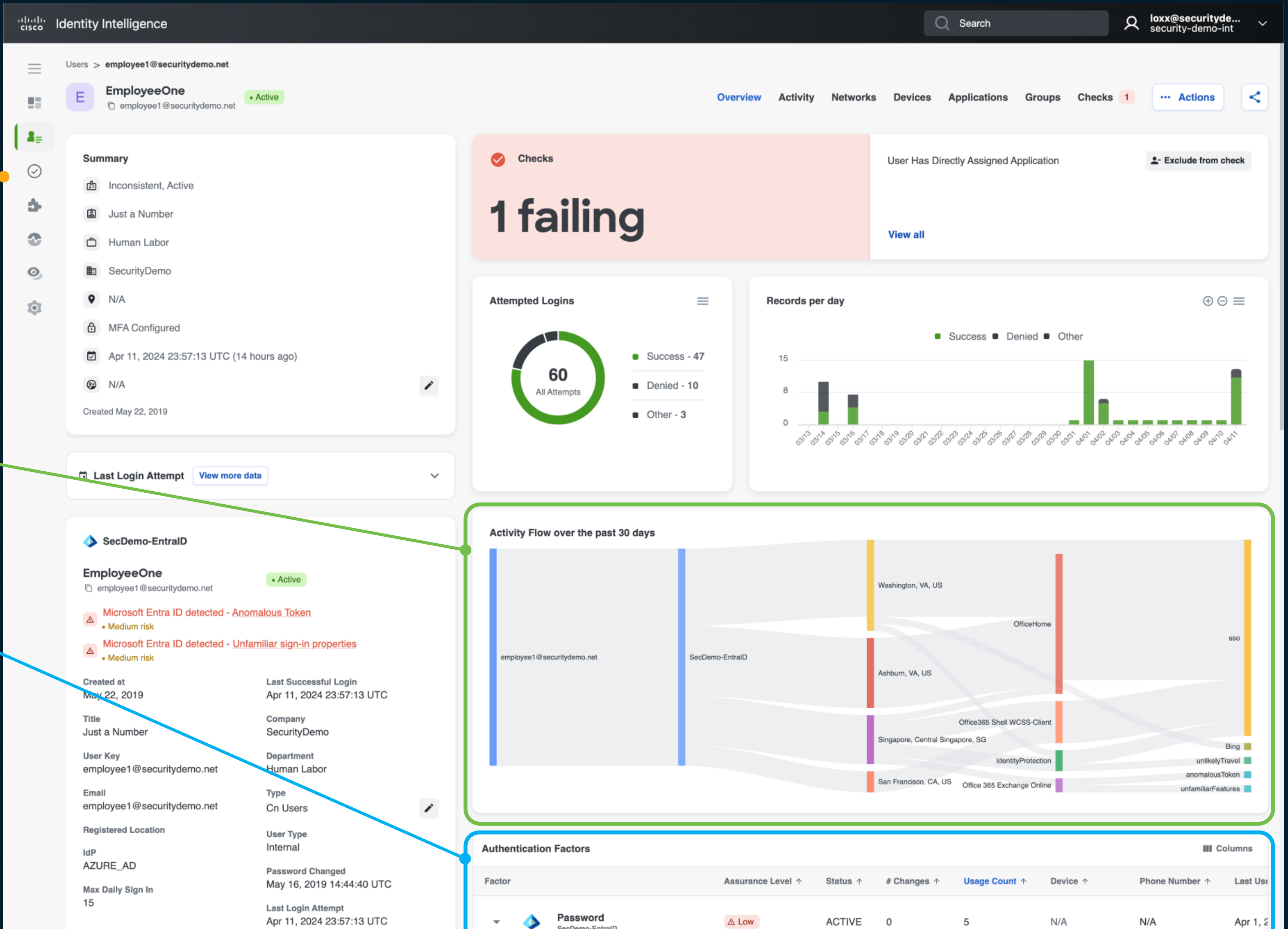
A true look at the user's identity related security, activity and other important properties.

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



Identity Intelligence

Search

loxx@securityde...
security-demo-int

Users > employee1@securitydemo.net

EmployeeOne • Active
employee1@securitydemo.net

Overview | Activity | Networks | Devices | Applications | Groups | Checks 1 | ··· Actions

Summary

- Inconsistent, Active
- Just a Number
- Human Labor
- SecurityDemo
- N/A
- MFA Configured
- Apr 11, 2024 23:57:13 UTC (14 hours ago)
- N/A

Created May 22, 2019

Checks

1 failing

User Has Directly Assigned Application

Exclude from check

View all

Attempted Logins

60
All Attempts

- Success - 47
- Denied - 10
- Other - 3

Records per day

Last Login Attempt | View more data

SecDemo-EntraID

EmployeeOne • Active
employee1@securitydemo.net

Microsoft Entra ID detected - Anomalous Token
• Medium risk

Microsoft Entra ID detected - Unfamiliar sign-in properties
• Medium risk

Created at May 22, 2019	Last Successful Login Apr 11, 2024 23:57:13 UTC
Title Just a Number	Company SecurityDemo
User Key employee1@securitydemo.net	Department Human Labor
Email employee1@securitydemo.net	Type Cn Users
Registered Location	User Type Internal
IdP AZURE_AD	Password Changed May 16, 2019 14:44:40 UTC
Max Daily Sign In 15	Last Login Attempt Apr 11, 2024 23:57:13 UTC

Activity Flow over the past 30 days

Authentication Factors

Columns

Factor	Assurance Level ↑	Status ↑	# Changes ↑	Usage Count ↑	Device ↑	Phone Number ↑	Last Use
Password SecDemo-EntraID	⚠ Low	ACTIVE	0	5	N/A	N/A	Apr 1, 2

cisco Live!

Activity

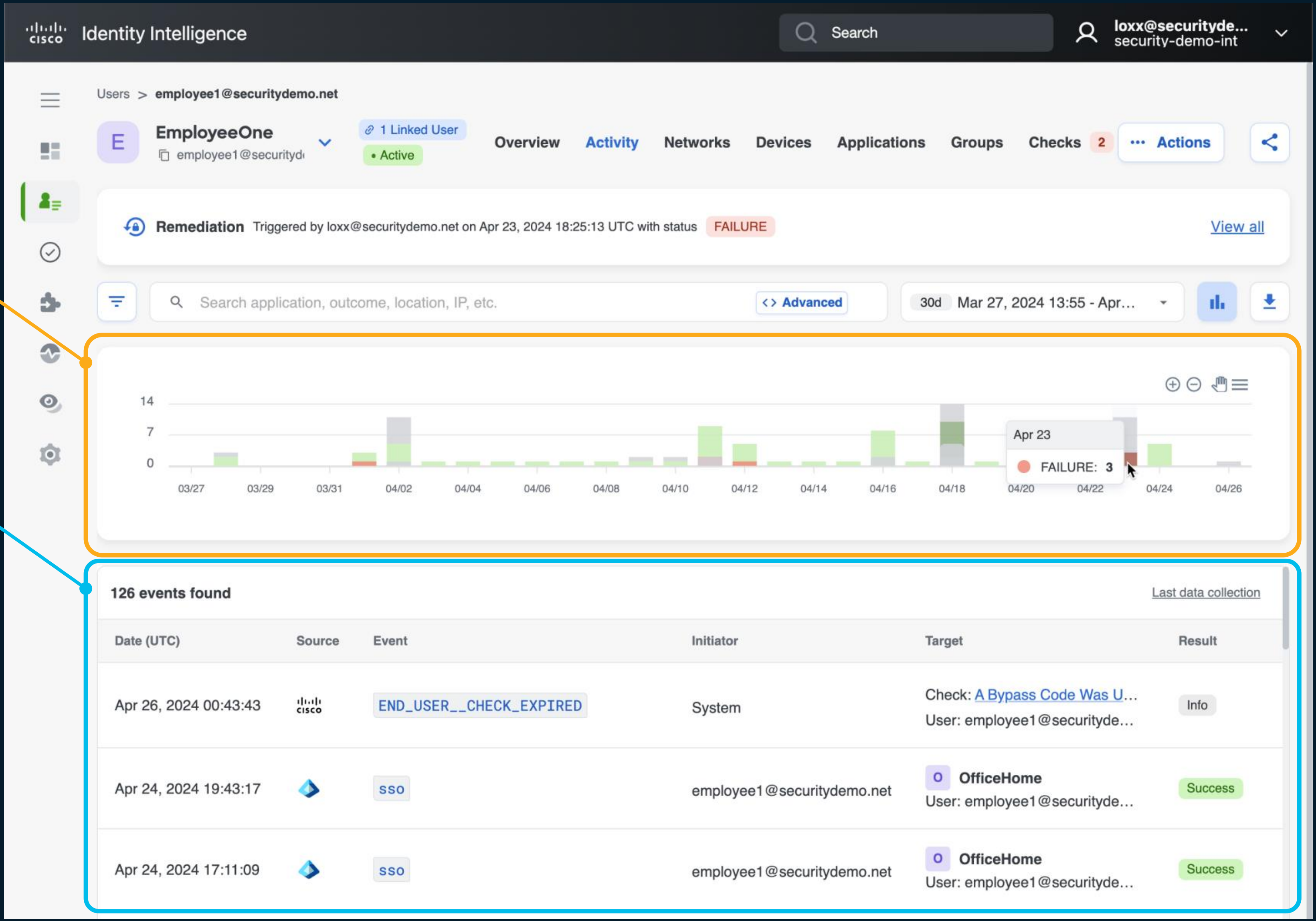
Activity Timeline

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



Identity Intelligence

Search

loxx@securityde...
security-demo-int

Users > employee1@securitydemo.net

EmployeeOne
employee1@securityd

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

Search application, outcome, location, IP, etc. <> Advanced 30d Mar 27, 2024 13:55 - Apr...

126 events found

Last data collection

Date (UTC)	Source	Event	Initiator	Target	Result
Apr 26, 2024 00:43:43	cisco	END_USER__CHECK_EXPIRED	System	Check: A Bypass Code Was U... User: employee1@securityde...	Info
Apr 24, 2024 19:43:17		SSO	employee1@securitydemo.net	O OfficeHome User: employee1@securityde...	Success
Apr 24, 2024 17:11:09		SSO	employee1@securitydemo.net	O OfficeHome User: employee1@securityde...	Success

Networks

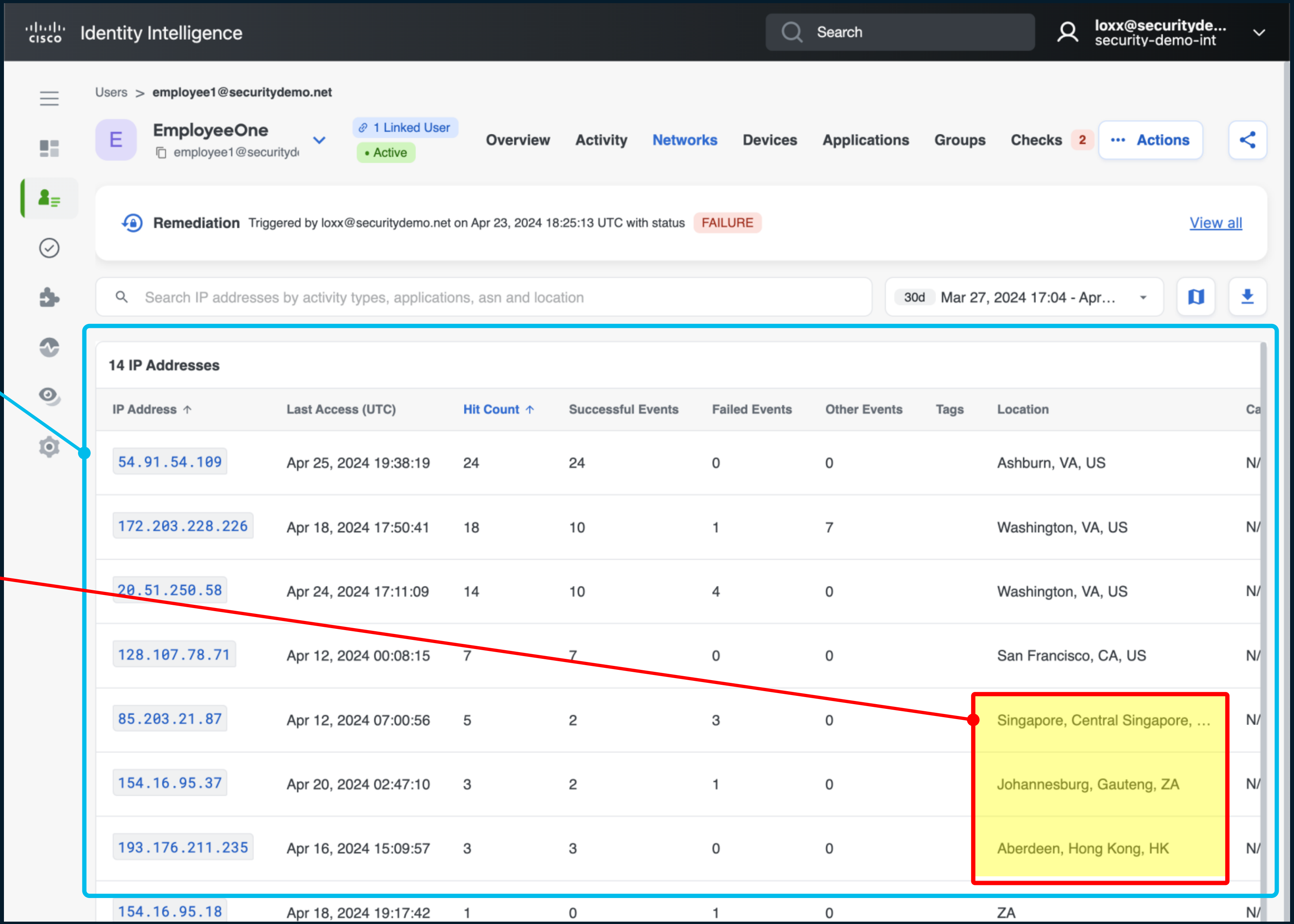
IP’s recorded in IDP Logs

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?


Identity Intelligence
Search
loxx@securityde...
security-demo-int
Users > employee1@securitydemo.net
E
EmployeeOne
employee1@securityd
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
Search IP addresses by activity types, applications, asn and location
30d Mar 27, 2024 17:04 - Apr...

14 IP Addresses

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

Devices

Devices from IDPs

Not all IDPs are created equal with device information

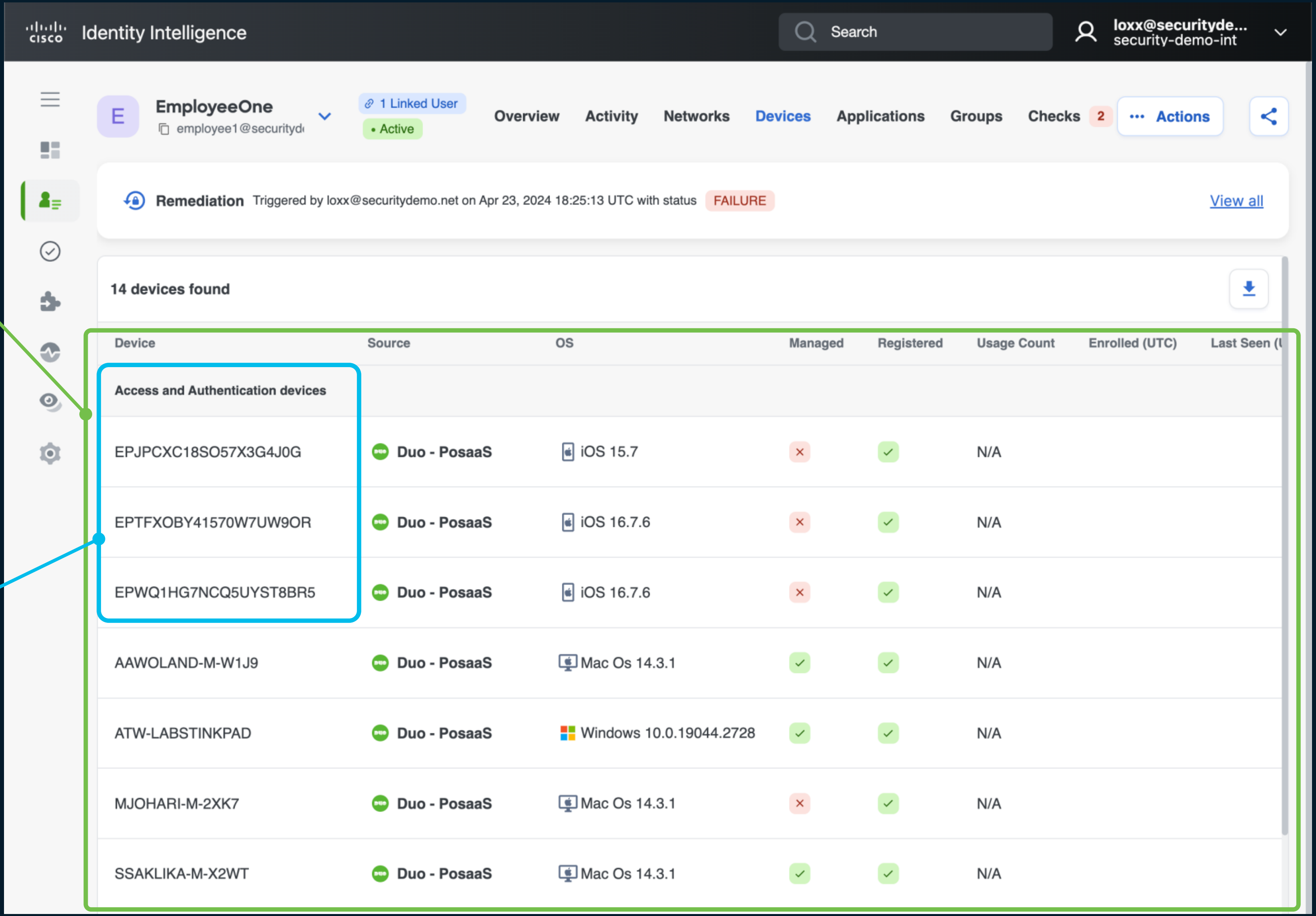
Duo is the best source for device data – when the Duo Auth includes the Health App.

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.



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 (U
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

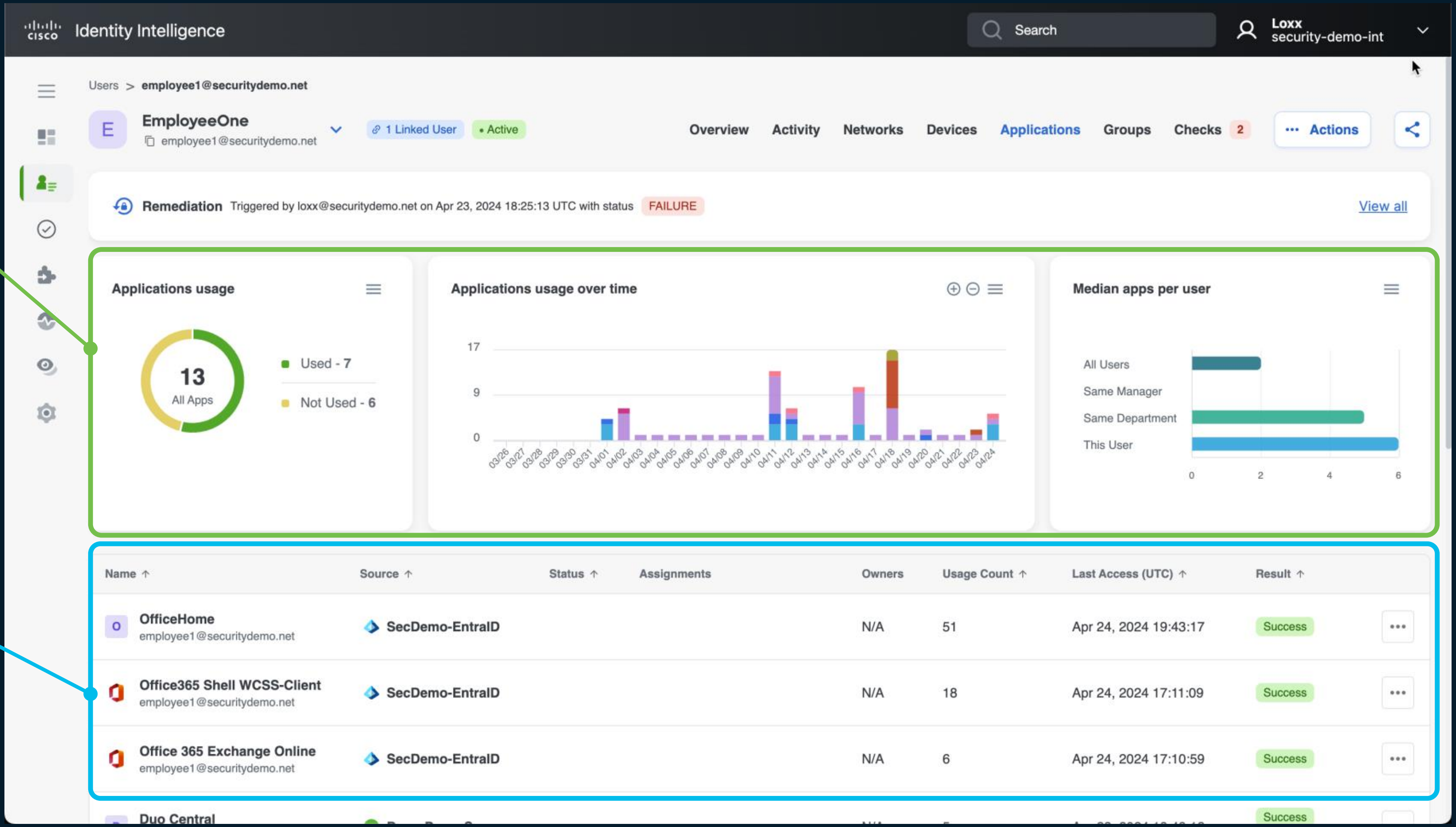
Quick overview of the apps used

Includes Apps not used

Application List

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

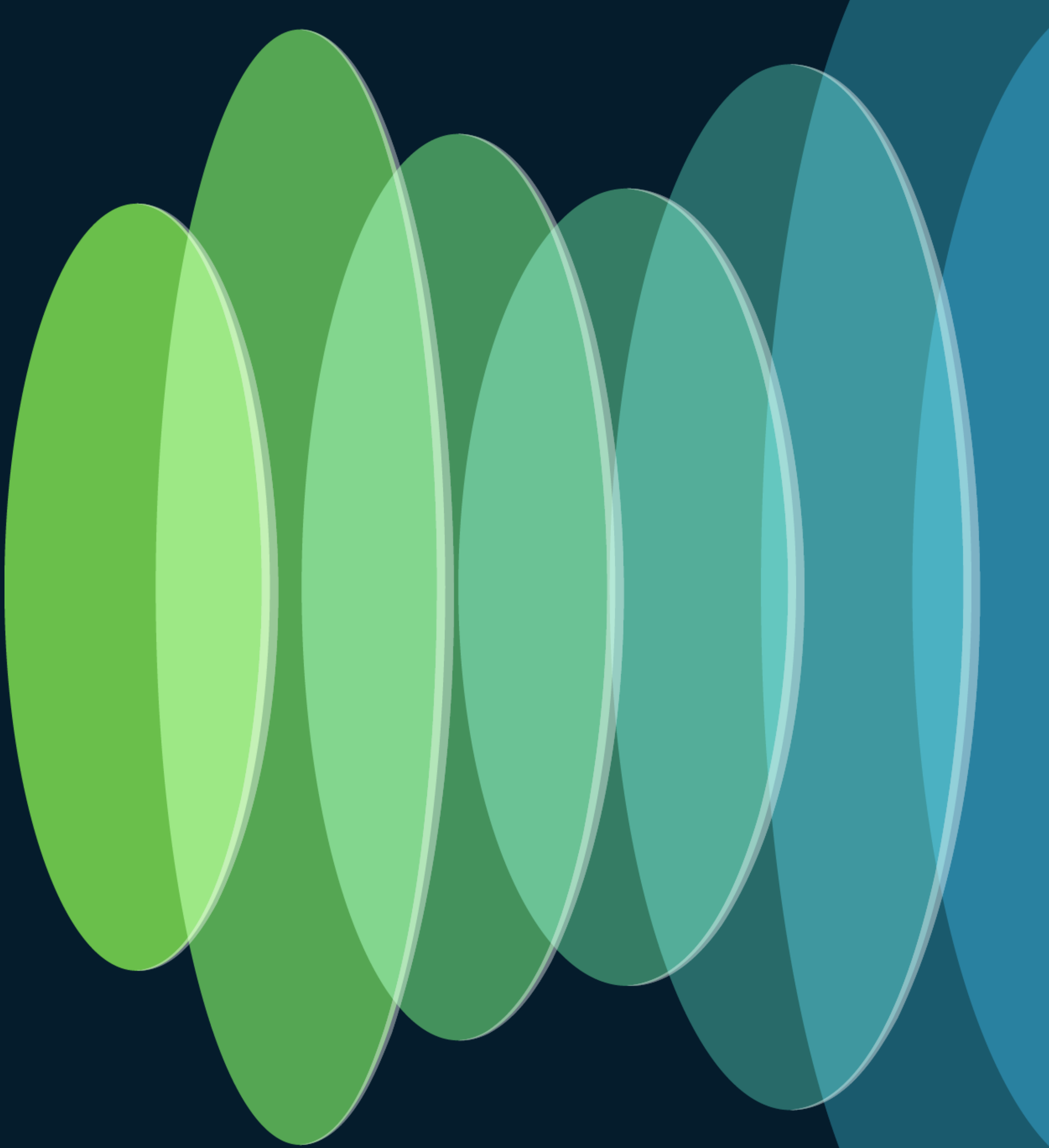
Which IDP reported the access & usage counts.



Remediation Triggered by loxx@securitydemo.net on Apr 23, 2024 18:25:13 UTC with status FAILURE View all

Name ↑	Source ↑	Status ↑	Assignments	Owners	Usage Count ↑	Last Access (UTC) ↑	Result ↑
OfficeHome employee1@securitydemo.net	SecDemo-EntraID			N/A	51	Apr 24, 2024 19:43:17	Success
Office365 Shell WCSS-Client employee1@securitydemo.net	SecDemo-EntraID			N/A	18	Apr 24, 2024 17:11:09	Success
Office 365 Exchange Online employee1@securitydemo.net	SecDemo-EntraID			N/A	6	Apr 24, 2024 17:10:59	Success
Duo Central							Success

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.

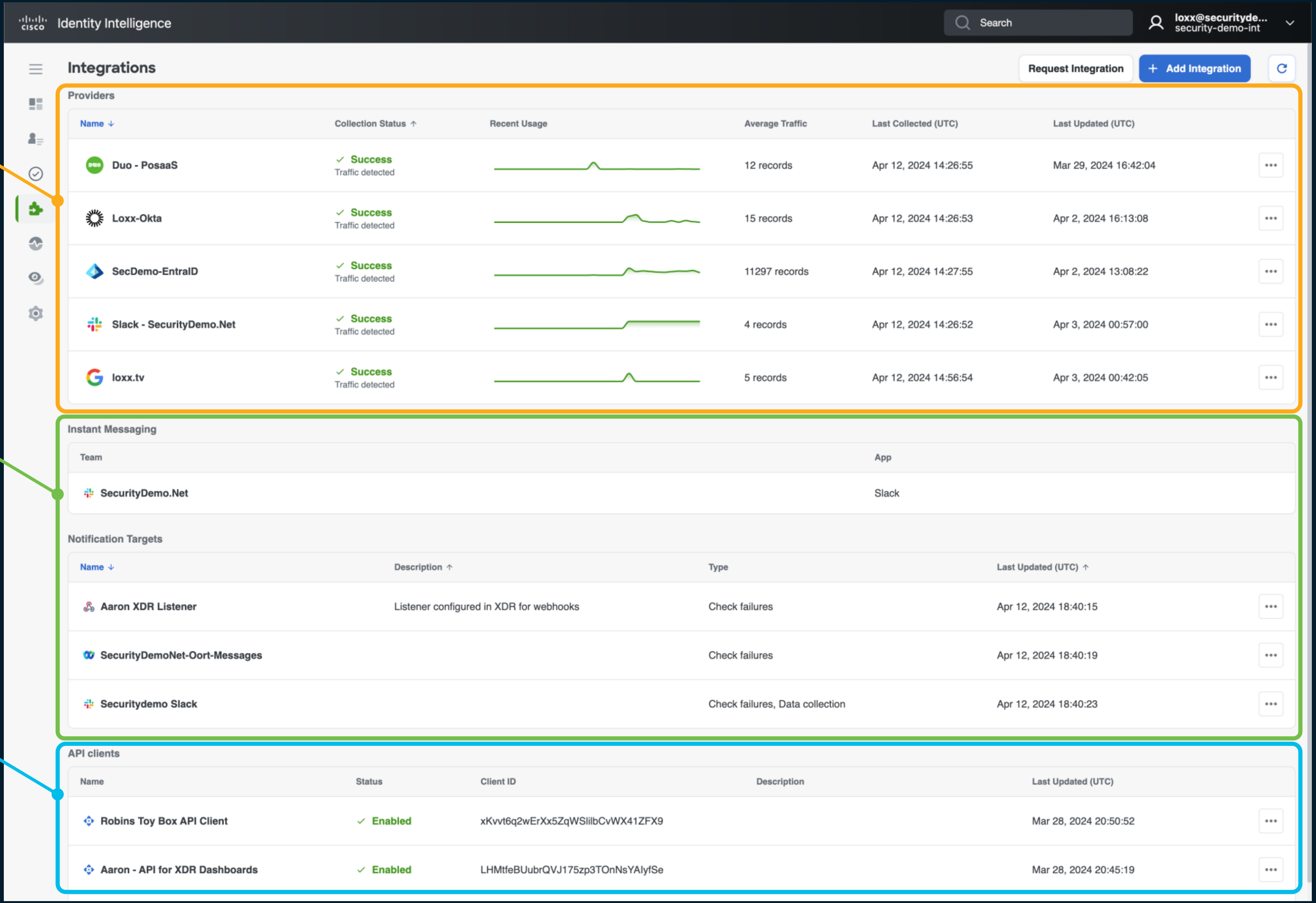
IM & Notification

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-Okta	✓ Success Traffic detected		15 records	Apr 12, 2024 14:26:53	Apr 2, 2024 16:13:08
SecDemo-EntraID	✓ 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	xKvvt6q2wErXx5ZqWSlilbCvWX41ZFX9		Mar 28, 2024 20:50:52
Aaron - API for XDR Dashboards	✓ Enabled	LHMtfeBUubrQVJ175zp3TOnNsYAlyfSe		Mar 28, 2024 20:45:19

Integrations are ”Life’s Blood” for CII

- Identity Intelligence is not an inline product
  - All CII’s information comes from integrations
  - CII integrates with Identity Providers, HRIS Systems and Applications
- Building the meta-directory of Users, Groups and Directory Structures
  - Uses APIs and Events
- Identifying Who is accessing What, from where and with which devices:
  - Authentication logs which can come across API syncs, or (preferably) streaming events
- Notifying users, administrators and investigators
  - CII integrates to send notices to email, collaboration tools, and SIEMs
- Some integrations are multi-purpose:
  - Slack is an IDP & a Notification System
  - Entra ID is required before you can add MS Teams as an integration source

Communication 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

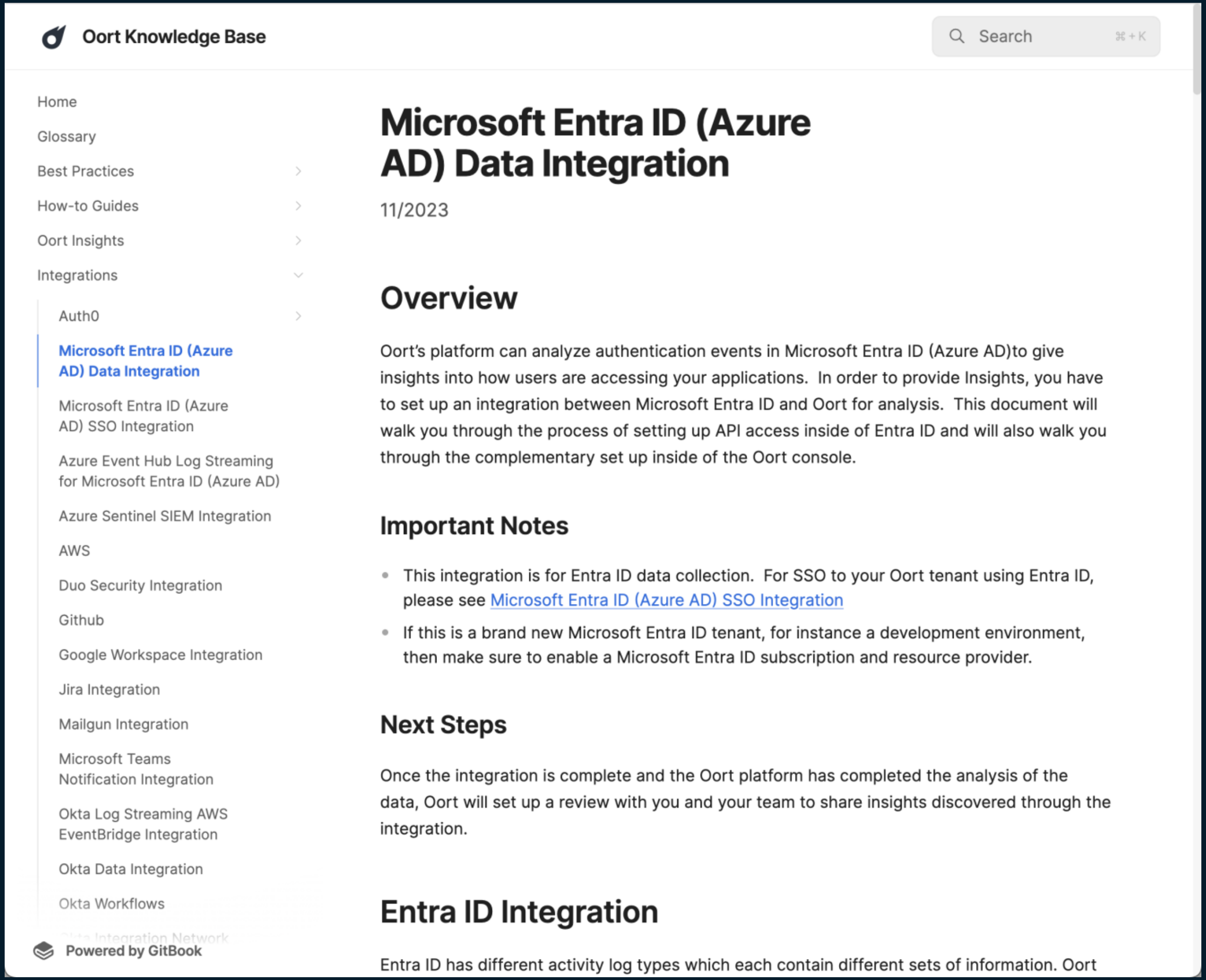
Identity Sources	Streaming	REST API Full Sync	REST API Delta Sync
Duo Security by Cisco	✓	✓	✓
Microsoft Entra (aka: Azure)	✓	✓	✓
Okta	✓	✓	✓
Slack[1]	X	✓	✓
Github	X	✓	✓
AWS	X	✓	✓
Google Workspace	X	✓	✓
Workday	X	✓	X
Salesforce	X	✓	partial
Auth0 (acquired by Okta)	✓	✓	X
Manual Upload (CSV/JSON)	X	X	X

[1] listed as notification, but does ID also

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 ownness of that portion on the vendor directly


Oort Knowledge Base
Search
⌘+K
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
Okta Integration Network
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.

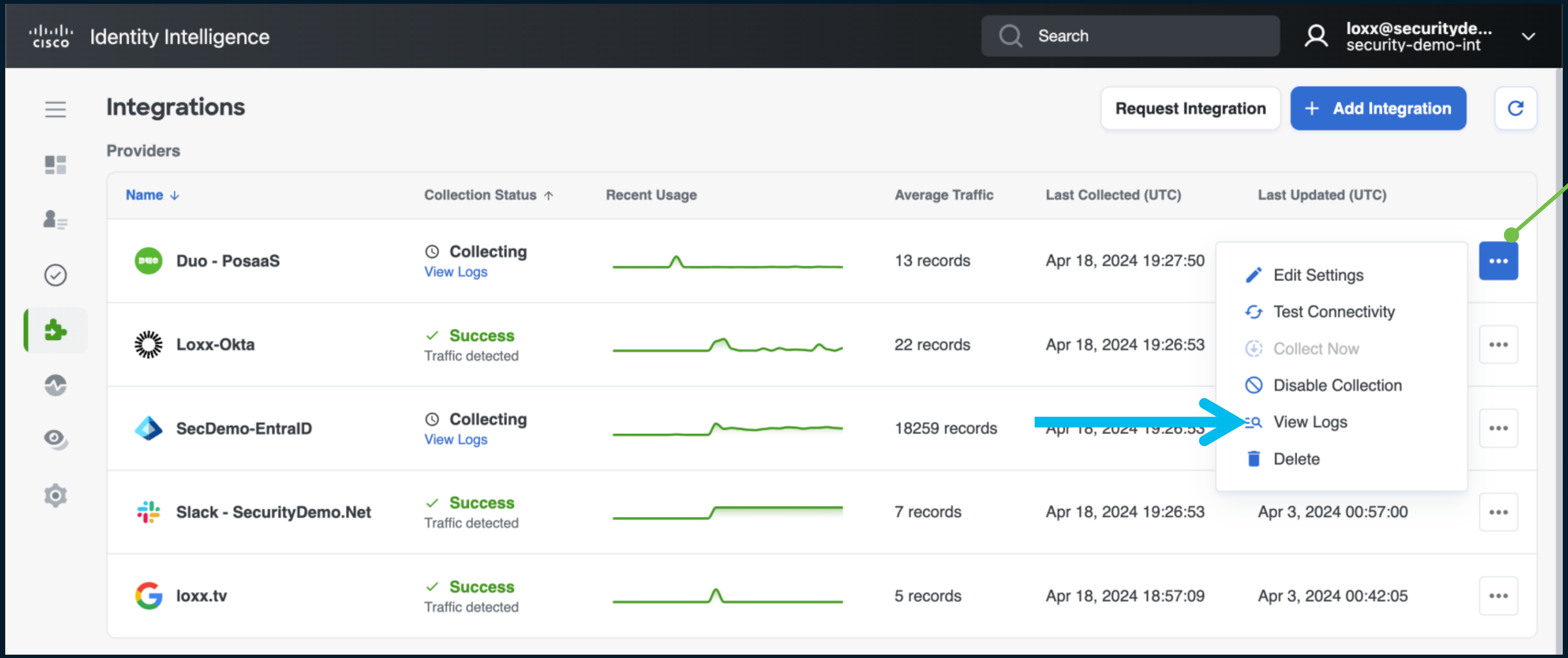
Next Steps

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



Integrations

Providers

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

Ellipses (...)

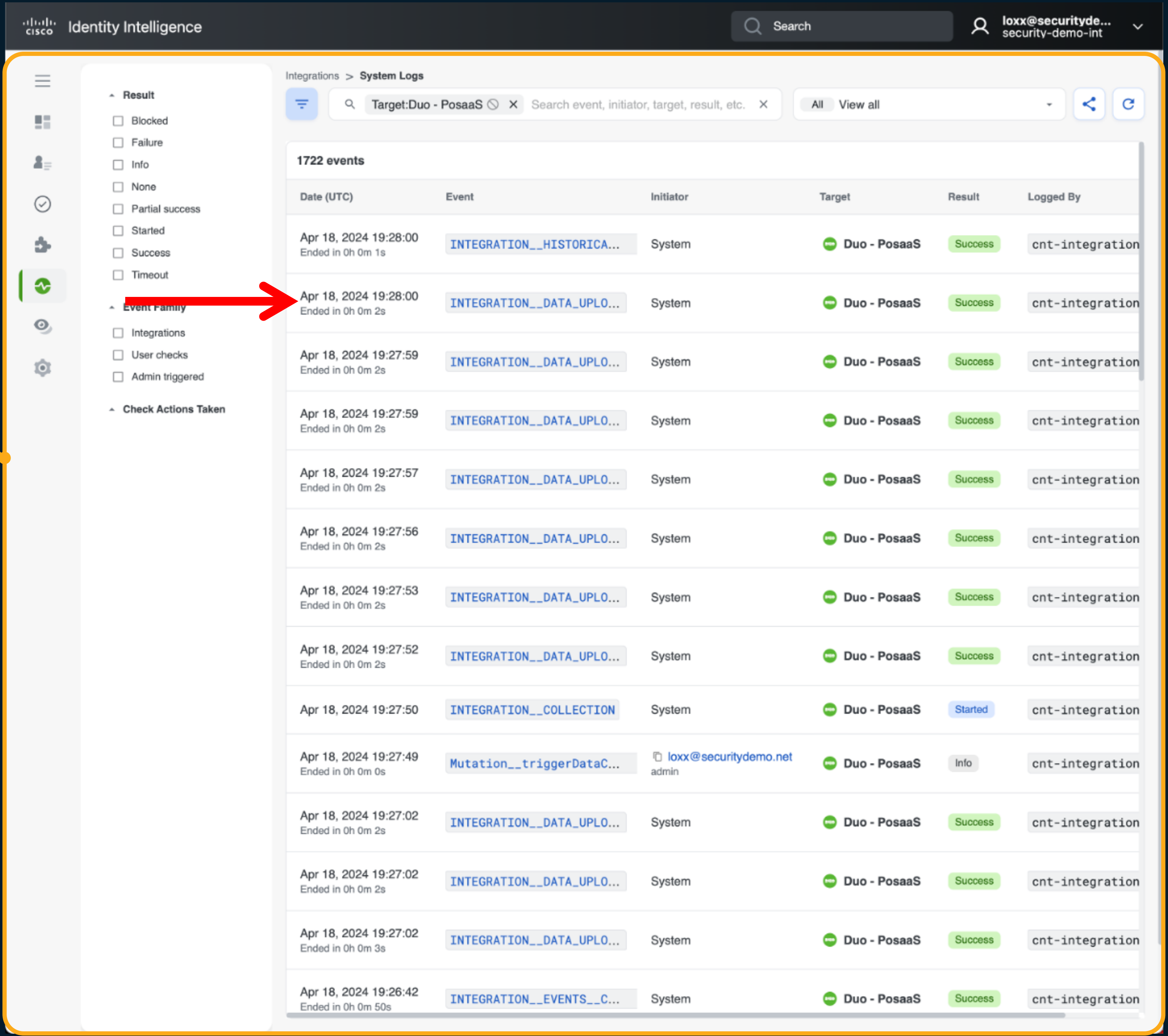
- Edit Settings
- Test connectivity – Terrific way to ensure the connection is working as expected
- Trigger collection (sync)
- Disable collection – use when there is an issue, and then enable again after that issue is resolved
- View Logs – see all logs related to the specific integration.
- Delete

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.



Integrations > System Logs

Target:Duo - PosaaS ✕ Search event, initiator, target, result, etc. ✕ All View all

Result

- ☐ Blocked
- ☐ Failure
- ☐ Info
- ☐ None
- ☐ Partial success
- ☐ Started
- ☐ Success
- ☐ Timeout

Event Family

- ☐ Integrations
- ☐ User checks
- ☐ Admin triggered

Check Actions Taken

1722 events

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

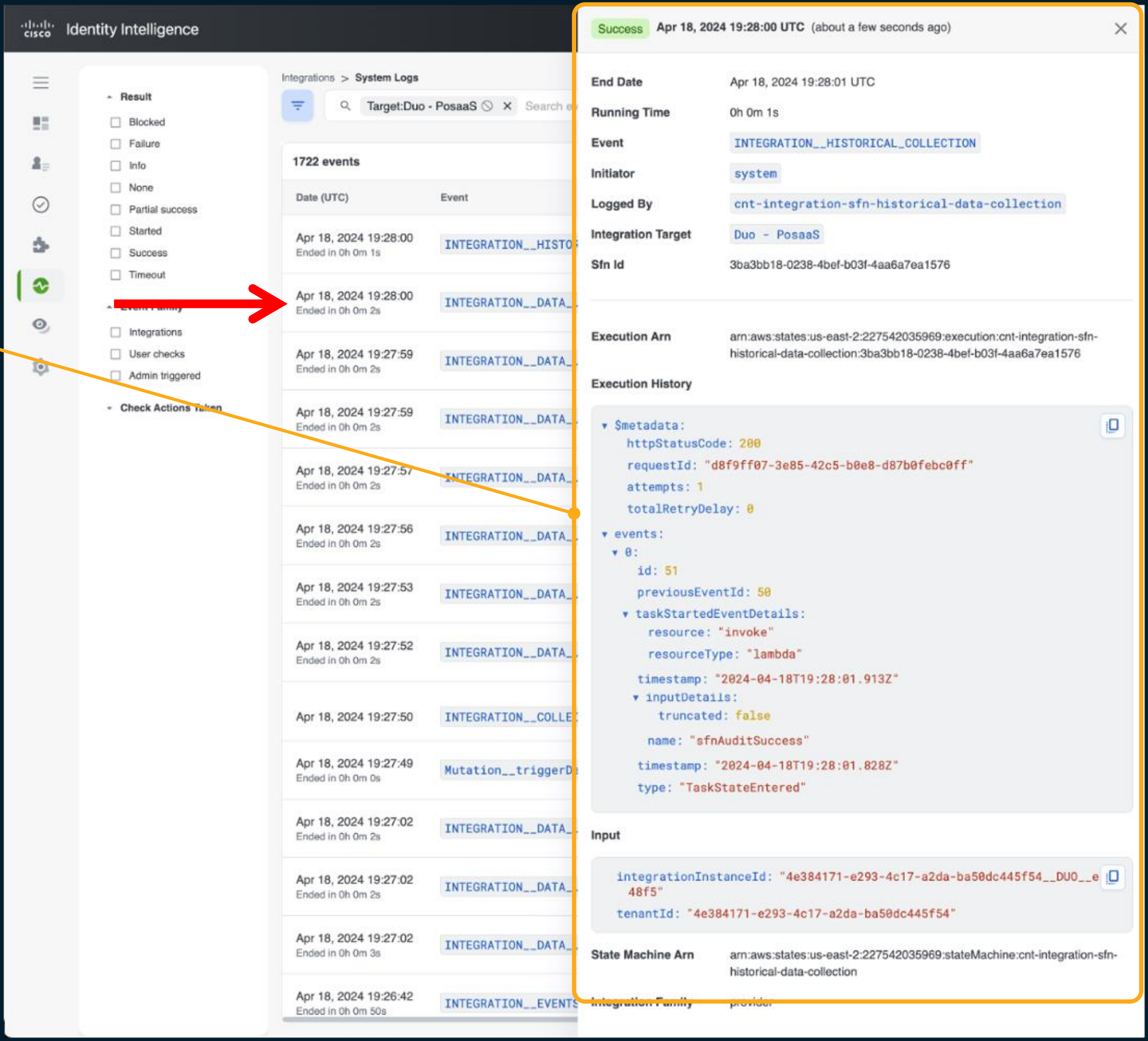
View Logs

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.

Aids tremendously when troubleshooting why information isn't getting sync'd across.



▴ Result
- ☐ Blocked
- ☐ Failure
- ☐ Info
- ☐ None
- ☐ Partial success
- ☐ Started
- ☐ Success
- ☐ Timeout

- ☐ Integrations
- ☐ User checks
- ☐ Admin triggered

▾ Check Actions Taken

1722 events

Date (UTC)	Event
Apr 18, 2024 19:28:00 Ended in 0h 0m 1s	INTEGRATION__HISTO
Apr 18, 2024 19:28:00 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:59 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:59 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:57 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:56 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:53 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:52 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:50	INTEGRATION__COLLE
Apr 18, 2024 19:27:49 Ended in 0h 0m 0s	Mutation__triggerD
Apr 18, 2024 19:27:02 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:02 Ended in 0h 0m 2s	INTEGRATION__DATA_
Apr 18, 2024 19:27:02 Ended in 0h 0m 3s	INTEGRATION__DATA_
Apr 18, 2024 19:26:42 Ended in 0h 0m 50s	INTEGRATION__EVENTS

Success Apr 18, 2024 19:28:00 UTC (about a few seconds ago)

End Date	Apr 18, 2024 19:28:01 UTC
Running Time	0h 0m 1s
Event	INTEGRATION__HISTORICAL_COLLECTION
Initiator	system
Logged By	cnt-integration-sfn-historical-data-collection
Integration Target	Duo - PosaaS
Sfn Id	3ba3bb18-0238-4bef-b03f-4aa6a7ea1576
Execution Arn	arn:aws:states:us-east-2:227542035969:execution:cnt-integration-sfn-historical-data-collection:3ba3bb18-0238-4bef-b03f-4aa6a7ea1576

Execution History

```
▾ $metadata:
    httpStatusCode: 200
    requestId: "d8f9ff07-3e85-42c5-b0e8-d87b0febc0ff"
    attempts: 1
    totalRetryDelay: 0
▾ events:
  ▾ 0:
      id: 51
      previousEventId: 50
    ▾ taskStartedEventDetails:
        resource: "invoke"
        resourceType: "lambda"
      timestamp: "2024-04-18T19:28:01.913Z"
     ▾ inputDetails:
          truncated: false
        name: "sfnAuditSuccess"
      timestamp: "2024-04-18T19:28:01.828Z"
      type: "TaskStateEntered"
```

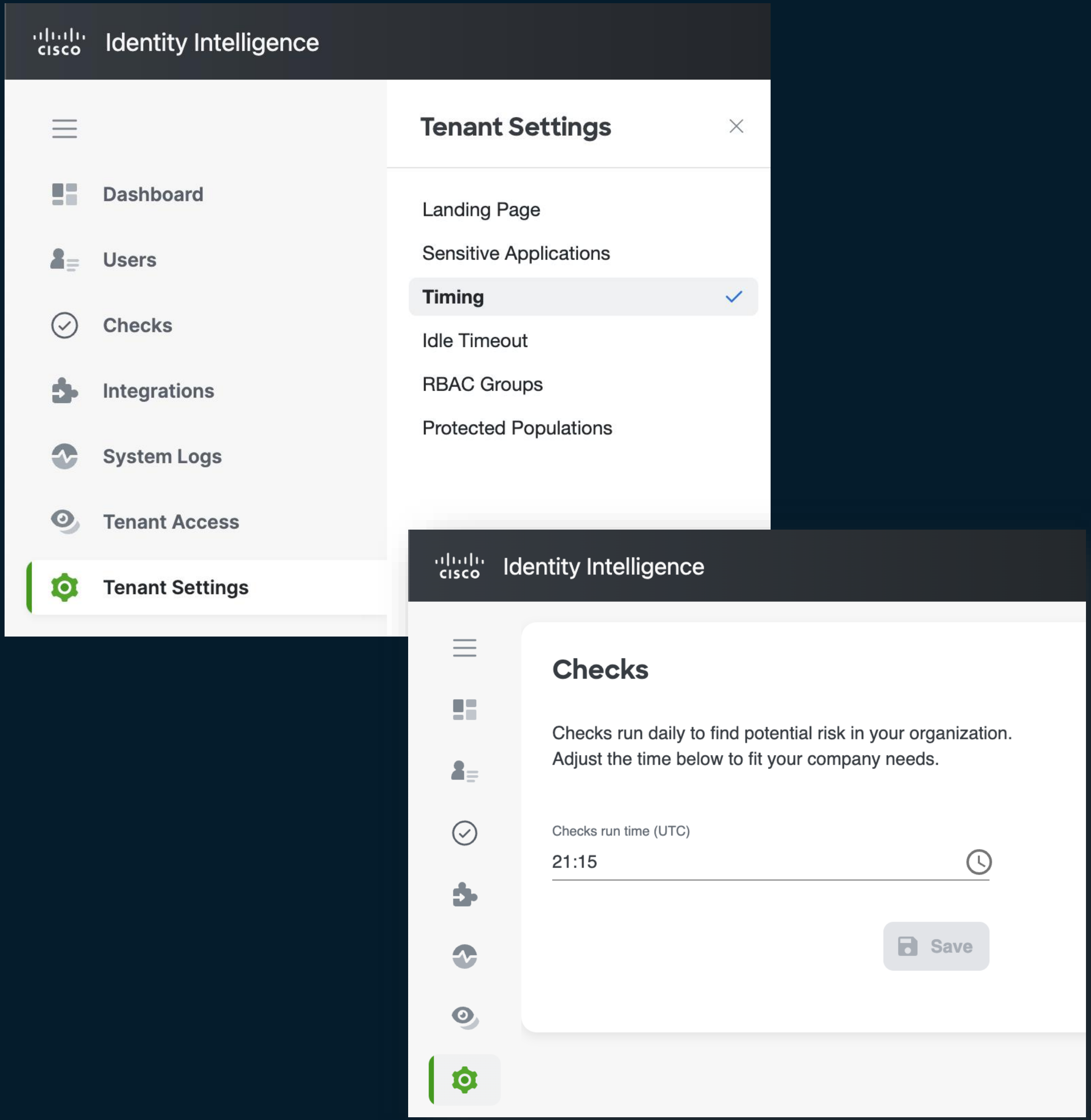
Input

```
integrationInstanceId: "4e384171-e293-4c17-a2da-ba50dc445f54__DUO__e
  48f5"
tenantId: "4e384171-e293-4c17-a2da-ba50dc445f54"
```

State Machine Arn	arn:aws:states:us-east-2:227542035969:stateMachine:cnt-integration-sfn-historical-data-collection
Integration Family	provider

Sync Schedule

- Tenant-level configuration
  - The time of day when the bulk sync requests are made via API's
  - The time is chosen by the system automatically after the first integration is added
  - If a different time is preferred for your organization, you may change it here
  - Note: This does not affect the streaming logs (Okta, EntraID, Duo & Auth0)



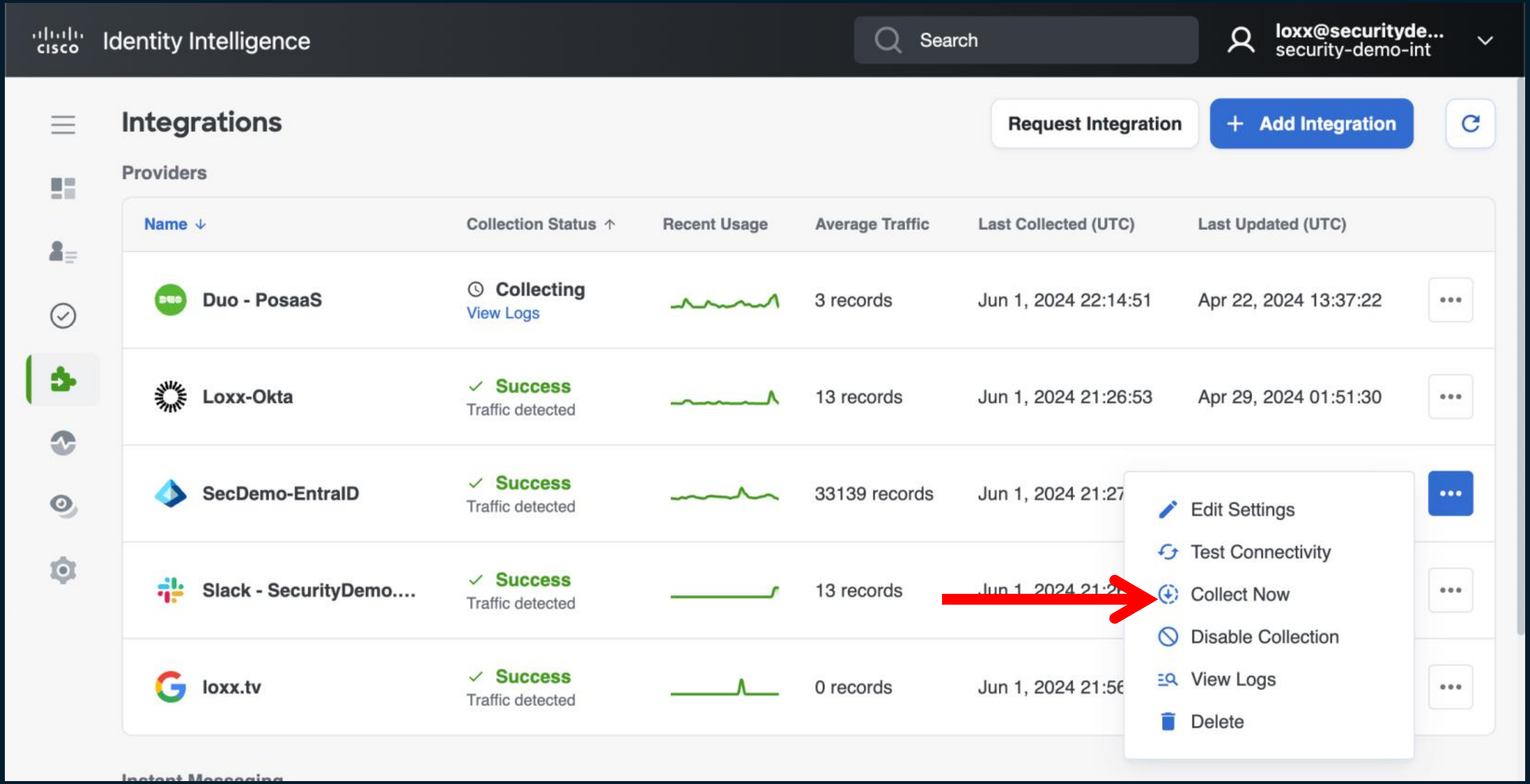
Checks

Checks run daily to find potential risk in your organization. Adjust the time below to fit your company needs.

Checks run time (UTC): 21:15

Sync Schedule

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



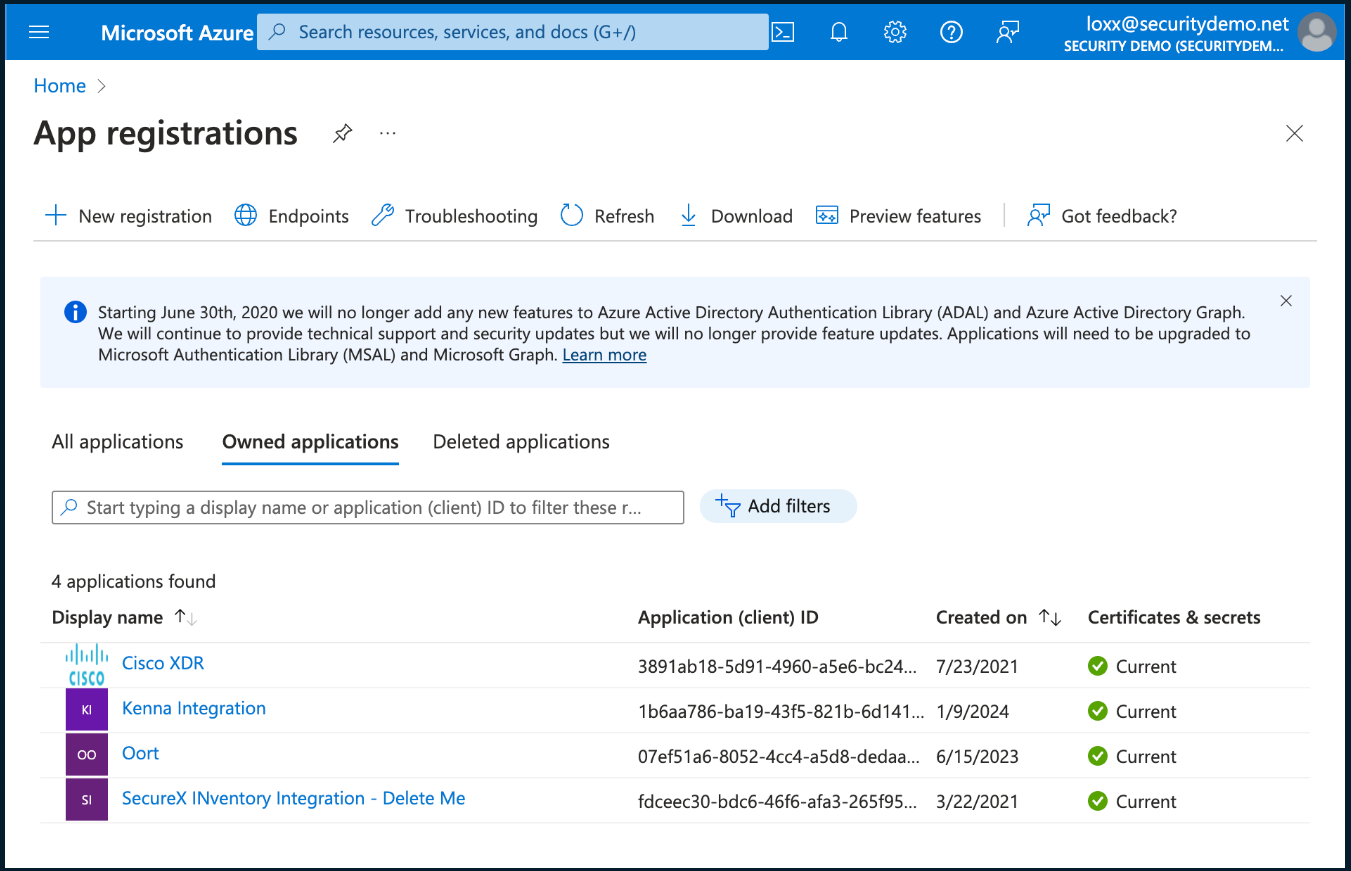
Name ↓	Collection Status ↑	Recent Usage	Average Traffic	Last Collected (UTC)	Last Updated (UTC)
Duo - PosaaS	Collecting View Logs		3 records	Jun 1, 2024 22:14:51	Apr 22, 2024 13:37:22
Loxx-Okta	✓ Success Traffic detected		13 records	Jun 1, 2024 21:26:53	Apr 29, 2024 01:51:30
SecDemo-EntraID	✓ Success Traffic detected		33139 records	Jun 1, 2024 21:27	
Slack - SecurityDemo....	✓ Success Traffic detected		13 records	Jun 1, 2024 21:2	
loxx.tv	✓ Success Traffic detected		0 records	Jun 1, 2024 21:56	

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



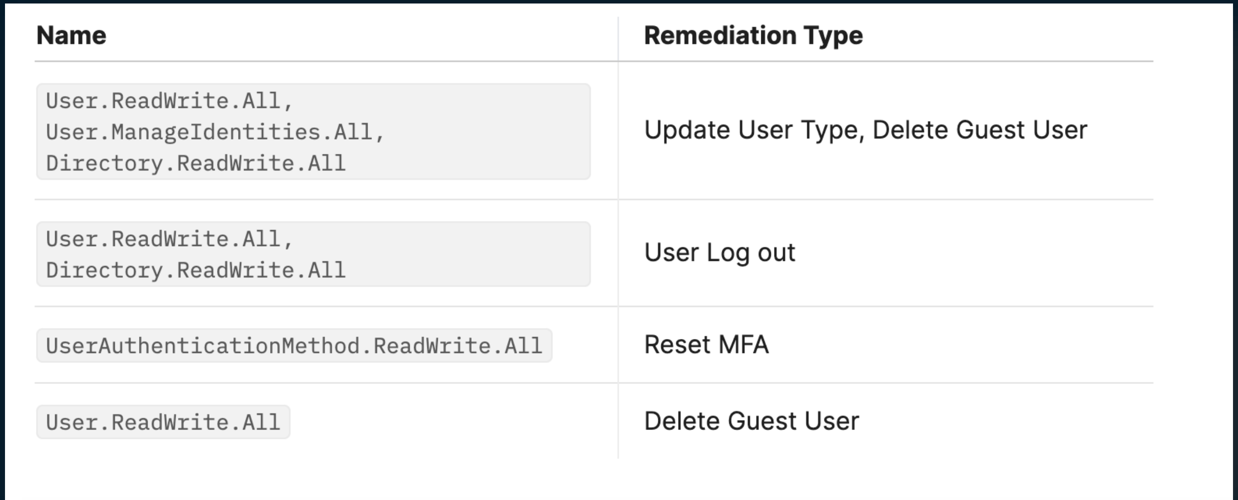
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

4 applications found

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

MS Entra ID

- Copies the directory data via the Graph API
- CII requires specific permissions
- Should setup event streaming for optimal integration
  - Customer needs to pay for a *subscription* for streamed events

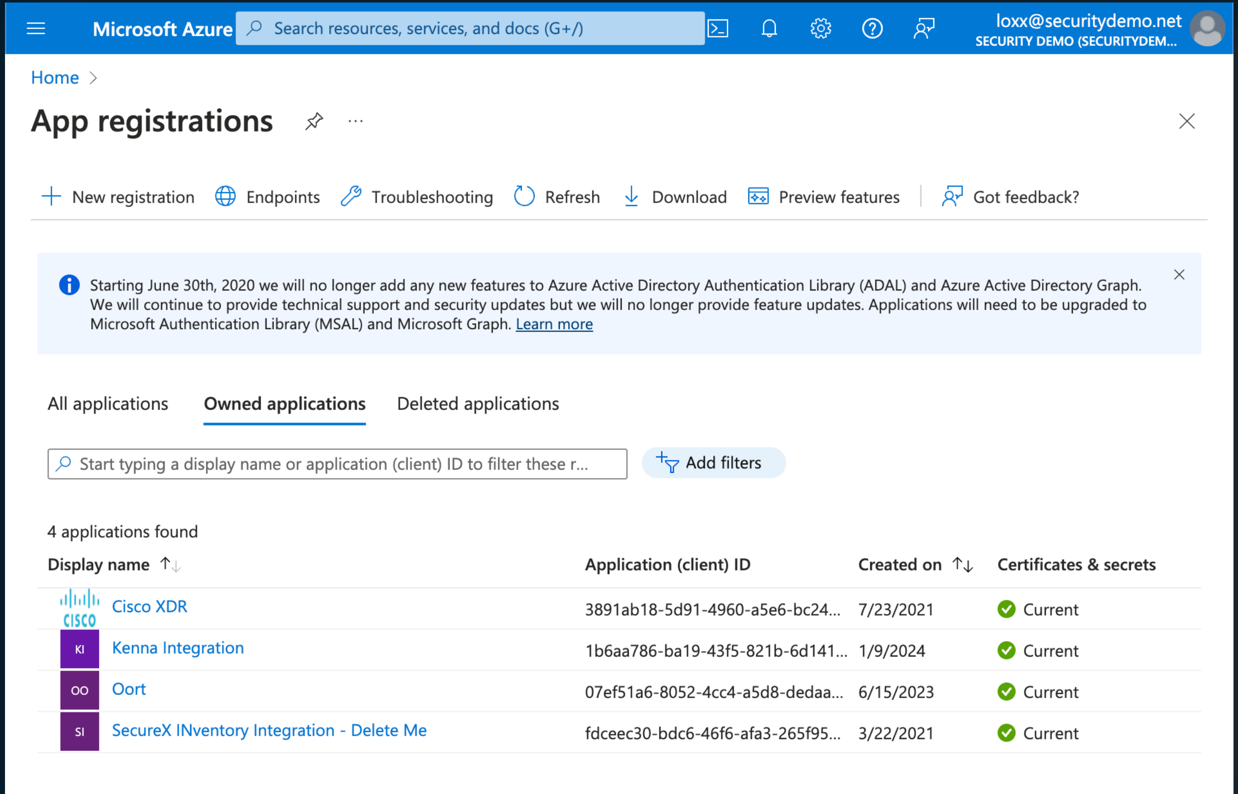


Name	Remediation Type

`User.ReadWrite.All,`
`User.ManageIdentities.All,`
`Directory.ReadWrite.All`
	Update User Type, Delete Guest User

`User.ReadWrite.All,`
`Directory.ReadWrite.All`
	User Log out

`UserAuthenticationMethod.ReadWrite.All`	Reset MFA
`User.ReadWrite.All`	Delete Guest User



Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

All applications
Owned applications
Deleted applications
Start typing a display name or application (client) ID to filter these r...
Add filters

4 applications found

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

MS Entra ID

General Settings

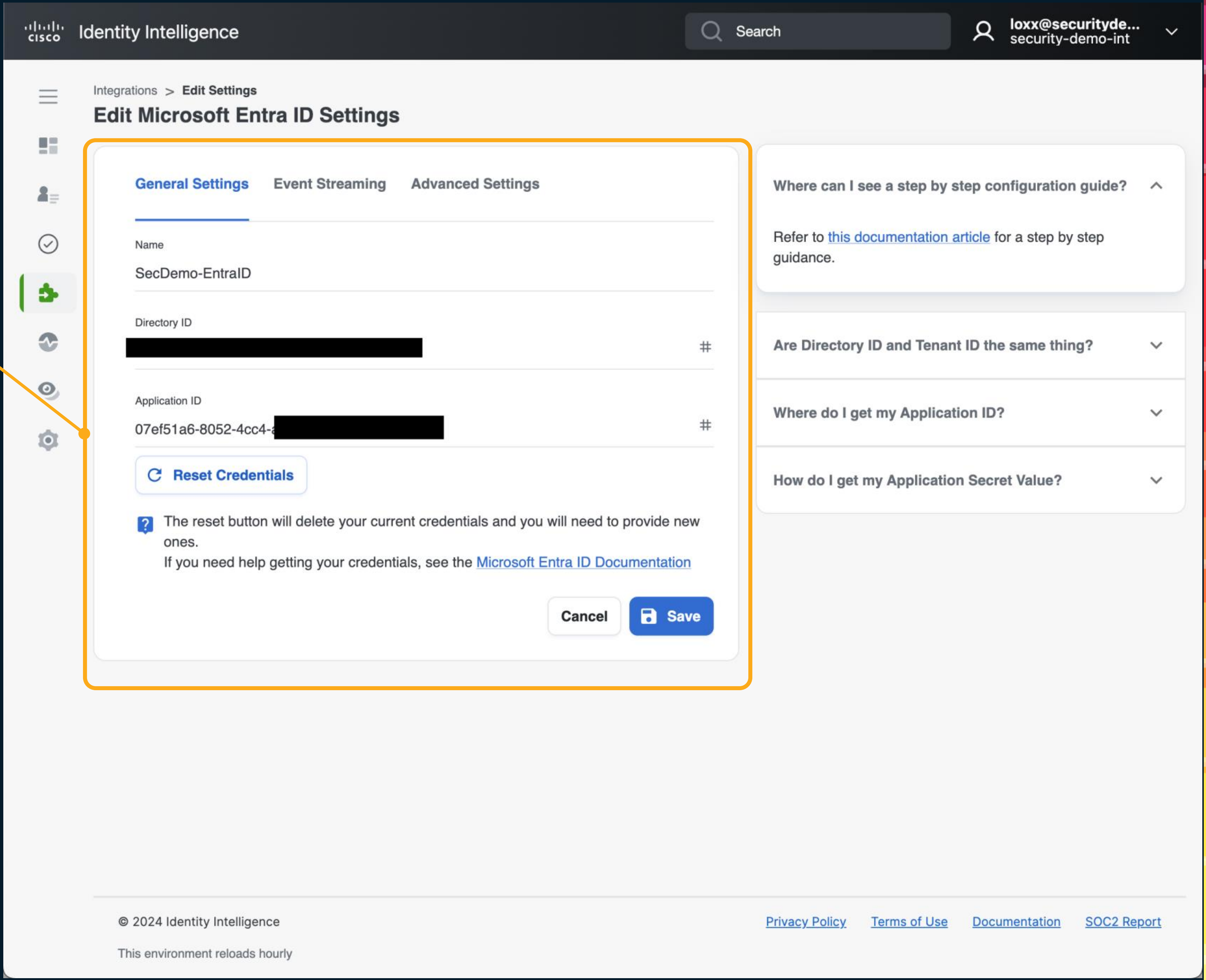
The credentials you obtained from the Azure "App" (ClientID, Secret Key, etc.)

The directory structure and attributes will be sync'd across this connection. However:

Microsoft's Graph API is throttled extensively

CII will [sometimes] see a 429 error code or network timeouts

It is less-than-desirable to integrate with Azure only via the Graph API



Edit Microsoft Entra ID Settings

Name: SecDemo-EntraID

Directory ID: [redacted]

Application ID: 07ef51a6-8052-4cc4-[redacted]

The reset button will delete your current credentials and you will need to provide new ones.
If you need help getting your credentials, see the Microsoft Entra ID Documentation

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?

Where do I get my Application ID?

How do I get my Application Secret Value?

© 2024 Identity Intelligence

This environment reloads hourly

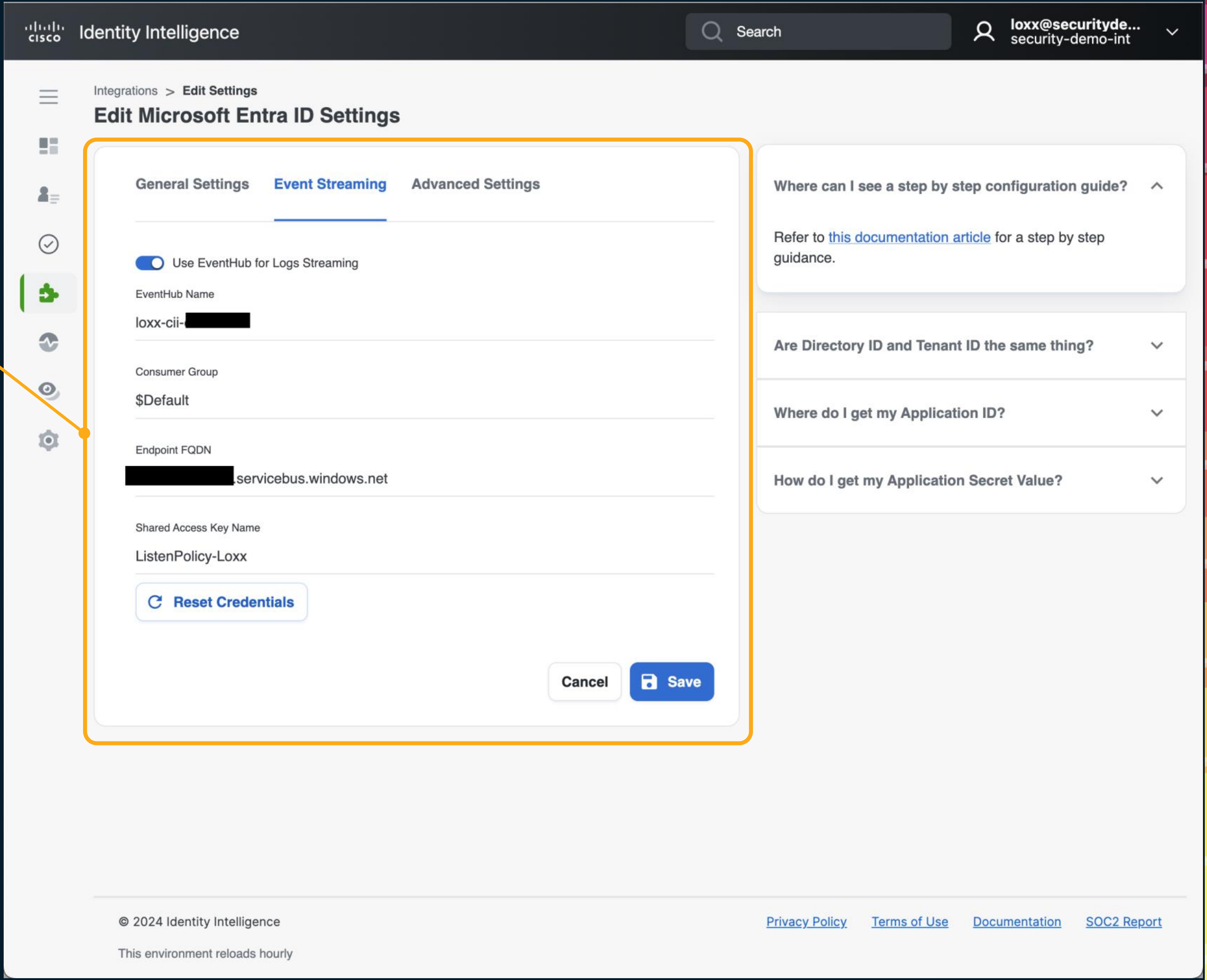
MS Entra ID

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)



Integrations > Edit Settings

Edit Microsoft Entra ID Settings

● Use EventHub for Logs Streaming

EventHub Name

loxx-cii-[redacted]

Consumer Group

$Default

Endpoint FQDN

[redacted].servicebus.windows.net

Shared Access Key Name

ListenPolicy-Loxx

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?

Where do I get my Application ID?

How do I get my Application Secret Value?

© 2024 Identity Intelligence

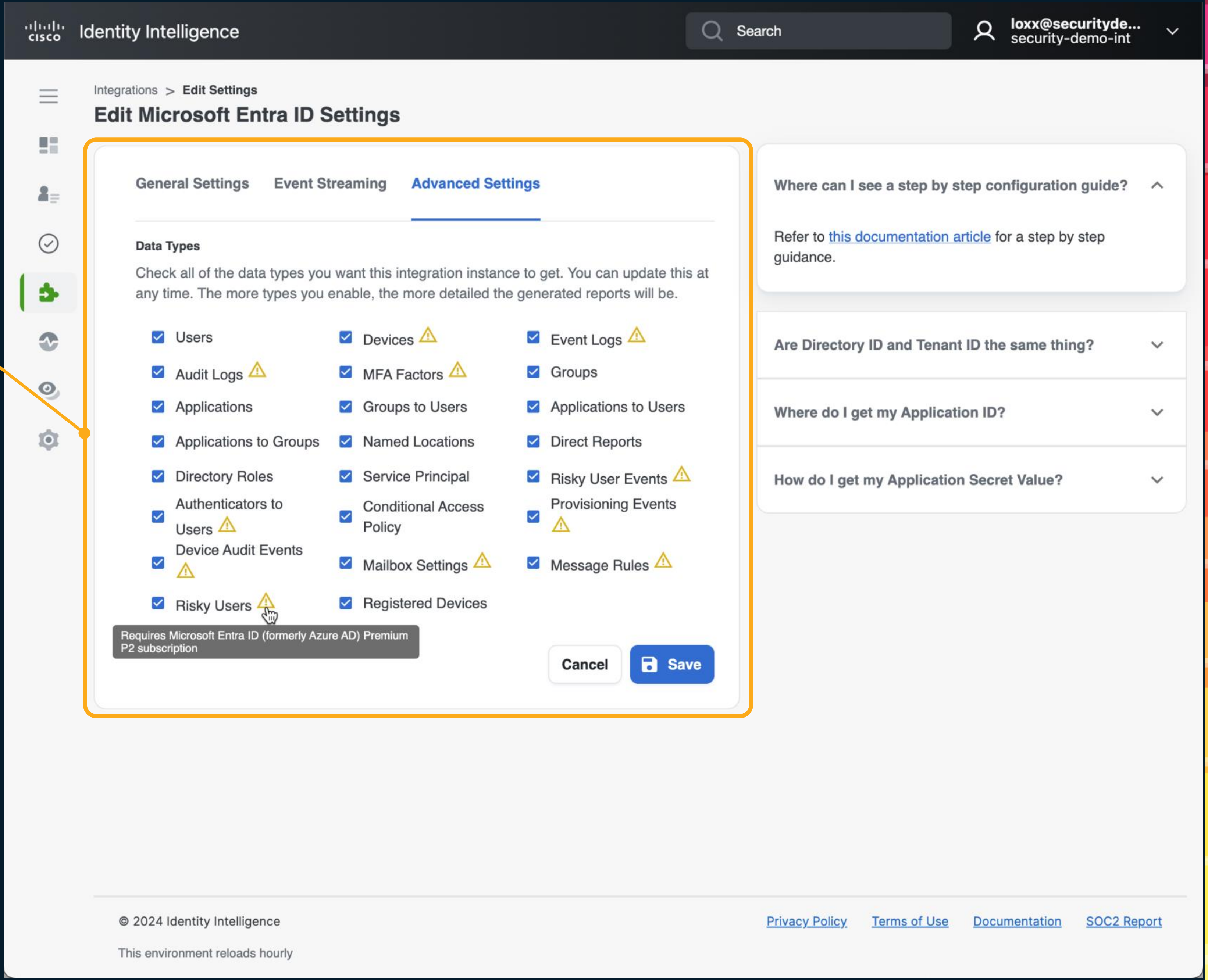
This environment reloads hourly

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.



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

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

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?

Where do I get my Application ID?

How do I get my Application Secret Value?

© 2024 Identity Intelligence

This environment reloads hourly

Okta Identity Engine

okta

Okta

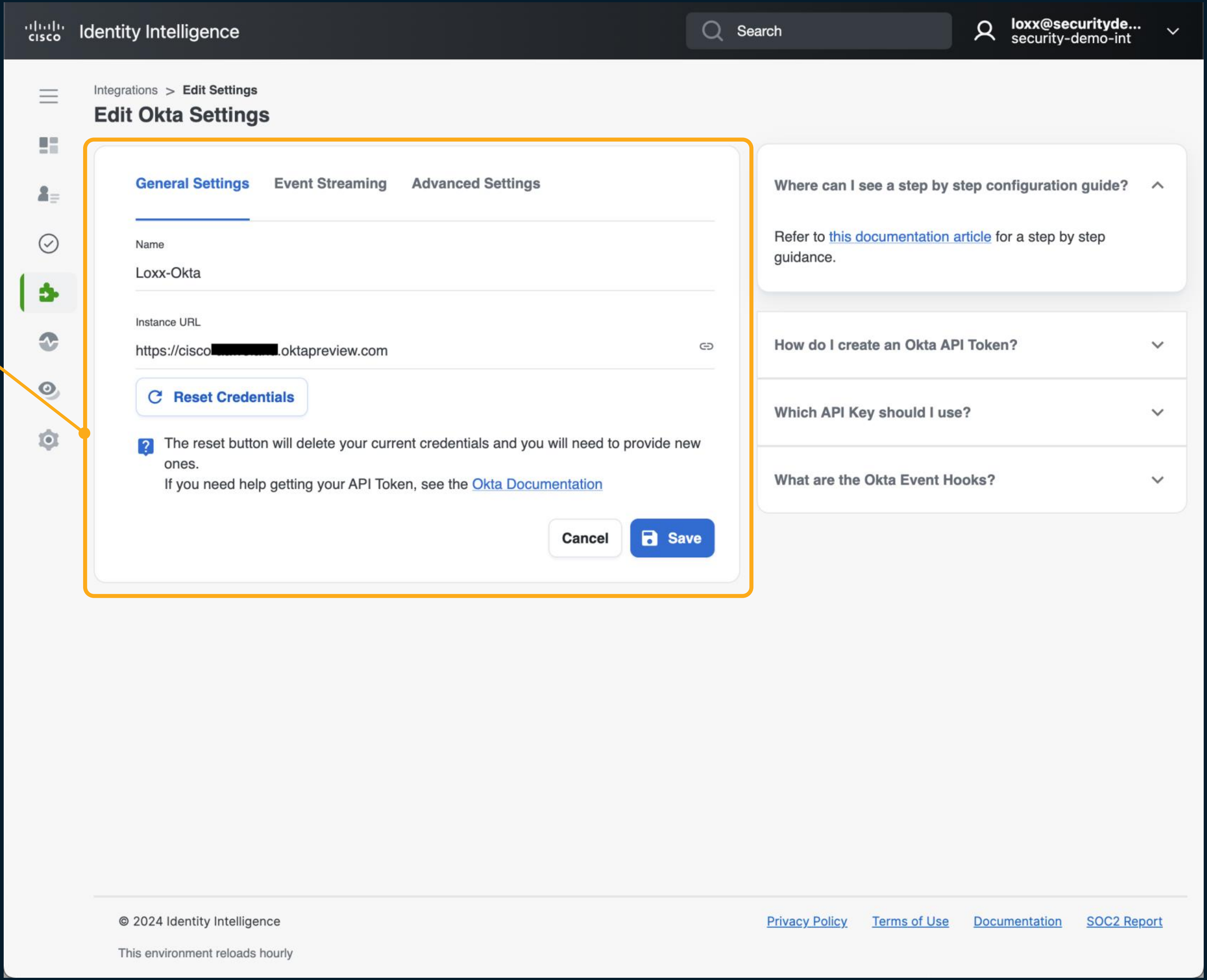
General Settings

The Okta integration requires the use of a service account in Okta.

In order to read all Okta data types, the service account will need BOTH Read-only Admin and Org Admin roles.

The service account is used to generate the API Token that is used for the integration, meaning the API calls are performed in the context of the service account.

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



Integrations > Edit Settings

Edit Okta Settings

Name: Loxx-Okta

Instance URL: https://cisco[redacted].oktapreview.com

The reset button will delete your current credentials and you will need to provide new ones.
If you need help getting your API Token, see the Okta Documentation

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?

Which API Key should I use?

What are the Okta Event Hooks?

© 2024 Identity Intelligence

This environment reloads hourly

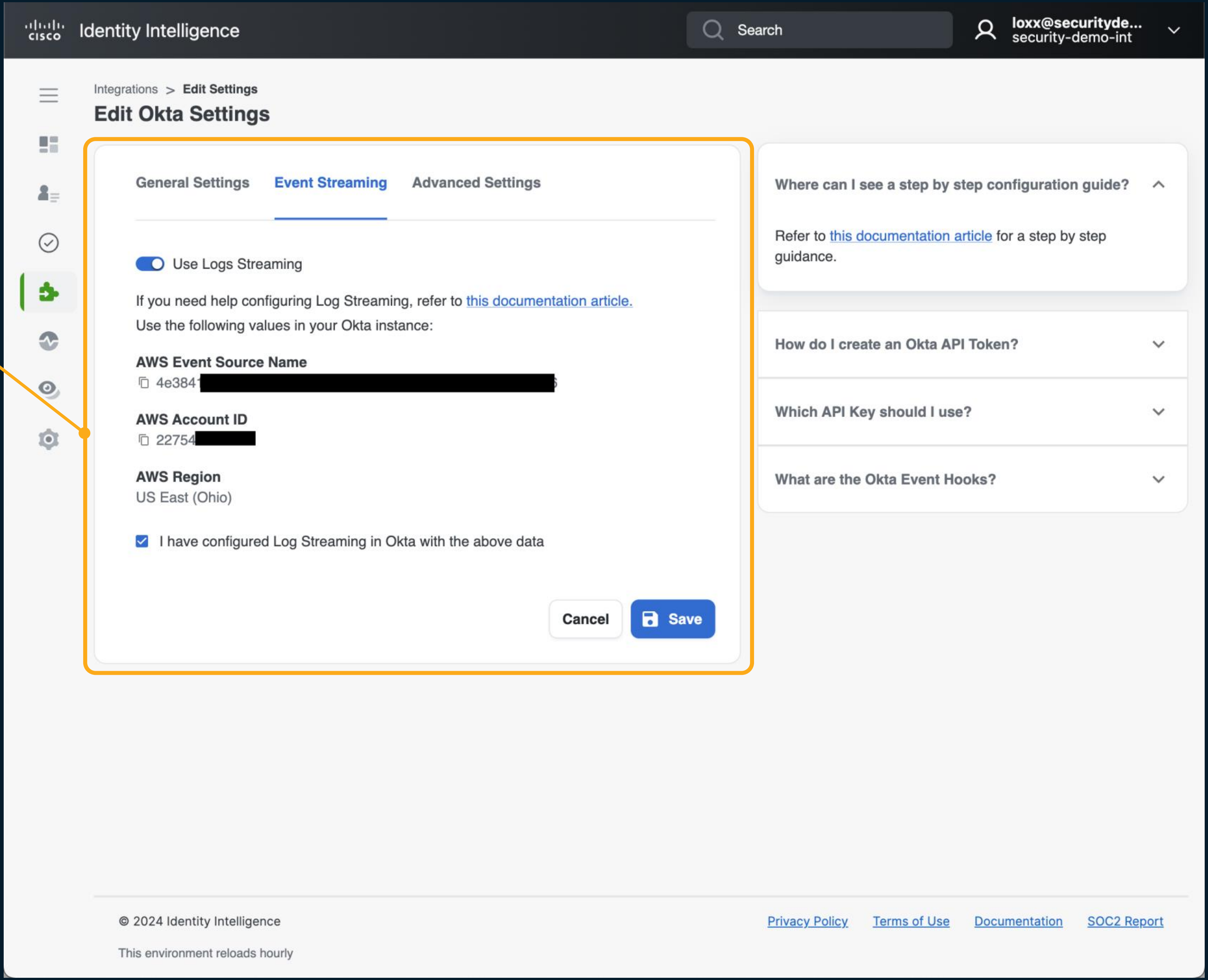
Okta

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?

Which API Key should I use?

What are the Okta Event Hooks?

© 2024 Identity Intelligence

This environment reloads hourly

Privacy Policy | Terms of Use | Documentation | SOC2 Report

Okta

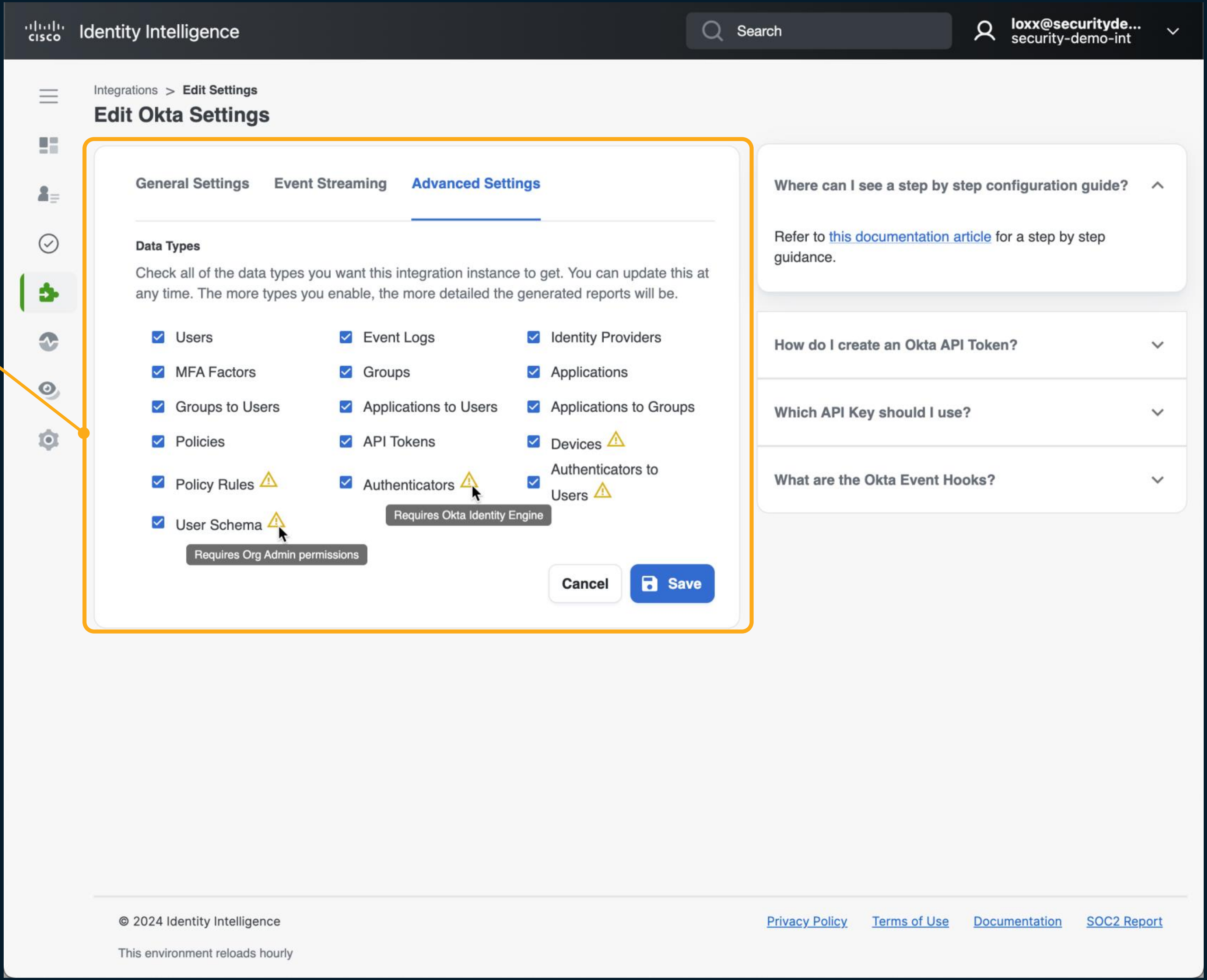
Advanced Settings

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.



Integrations > Edit Settings

Edit Okta 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
- ☑ MFA Factors
- ☑ Groups to Users
- ☑ Policies
- ☑ Policy Rules ⚠
- ☑ User Schema ⚠
- ☑ Event Logs
- ☑ Groups
- ☑ Applications to Users
- ☑ API Tokens
- ☑ Authenticators ⚠
- ☑ Identity Providers
- ☑ Applications
- ☑ Applications to Groups
- ☑ Devices ⚠
- ☑ Authenticators to Users ⚠

Requires Okta Identity Engine

Requires Org Admin permissions

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?

Which API Key should I use?

What are the Okta Event Hooks?

© 2024 Identity Intelligence

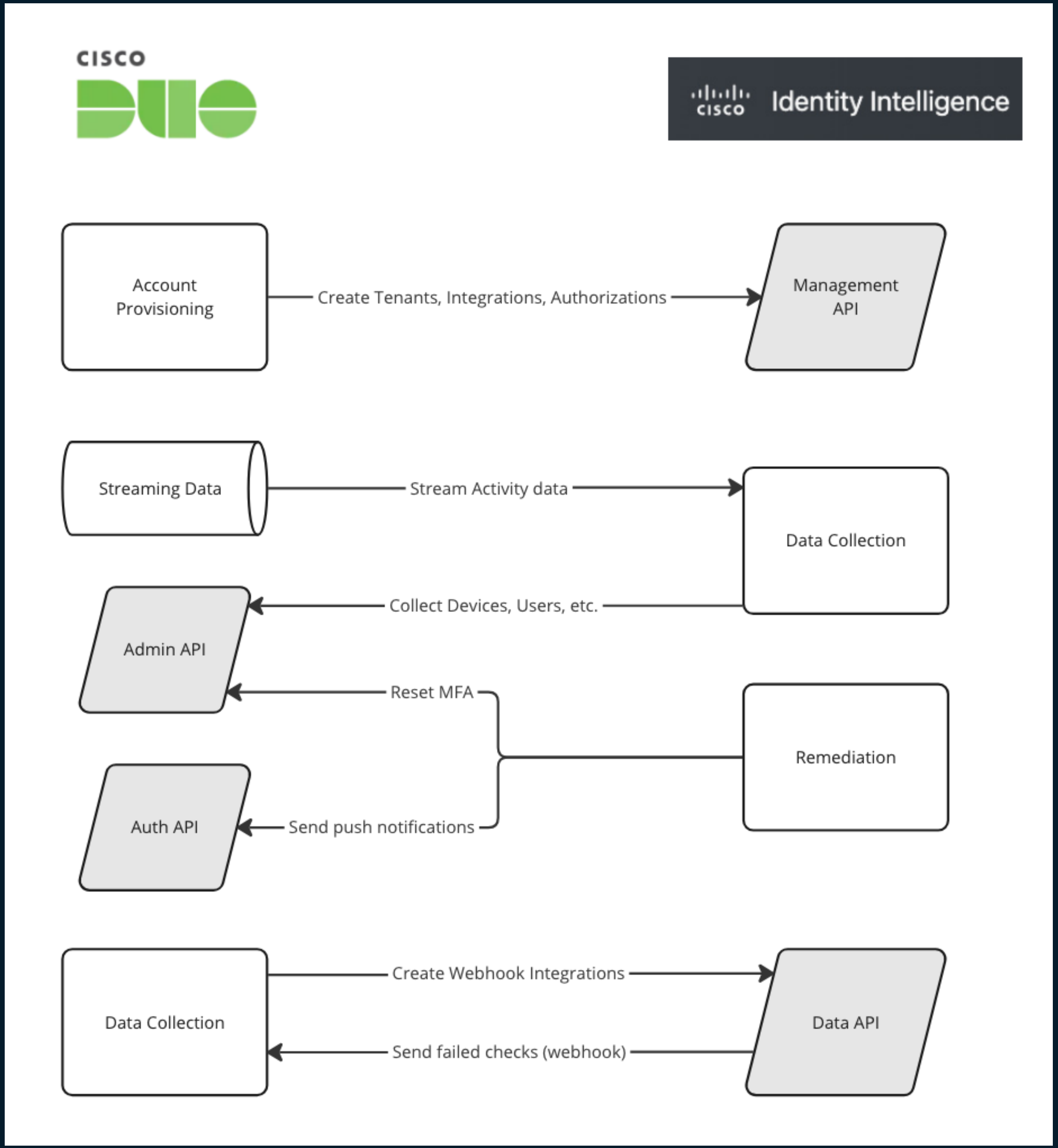
This environment reloads hourly

Cisco XDR
Splunk SOAR
etc.

Duo
a Cisco Company

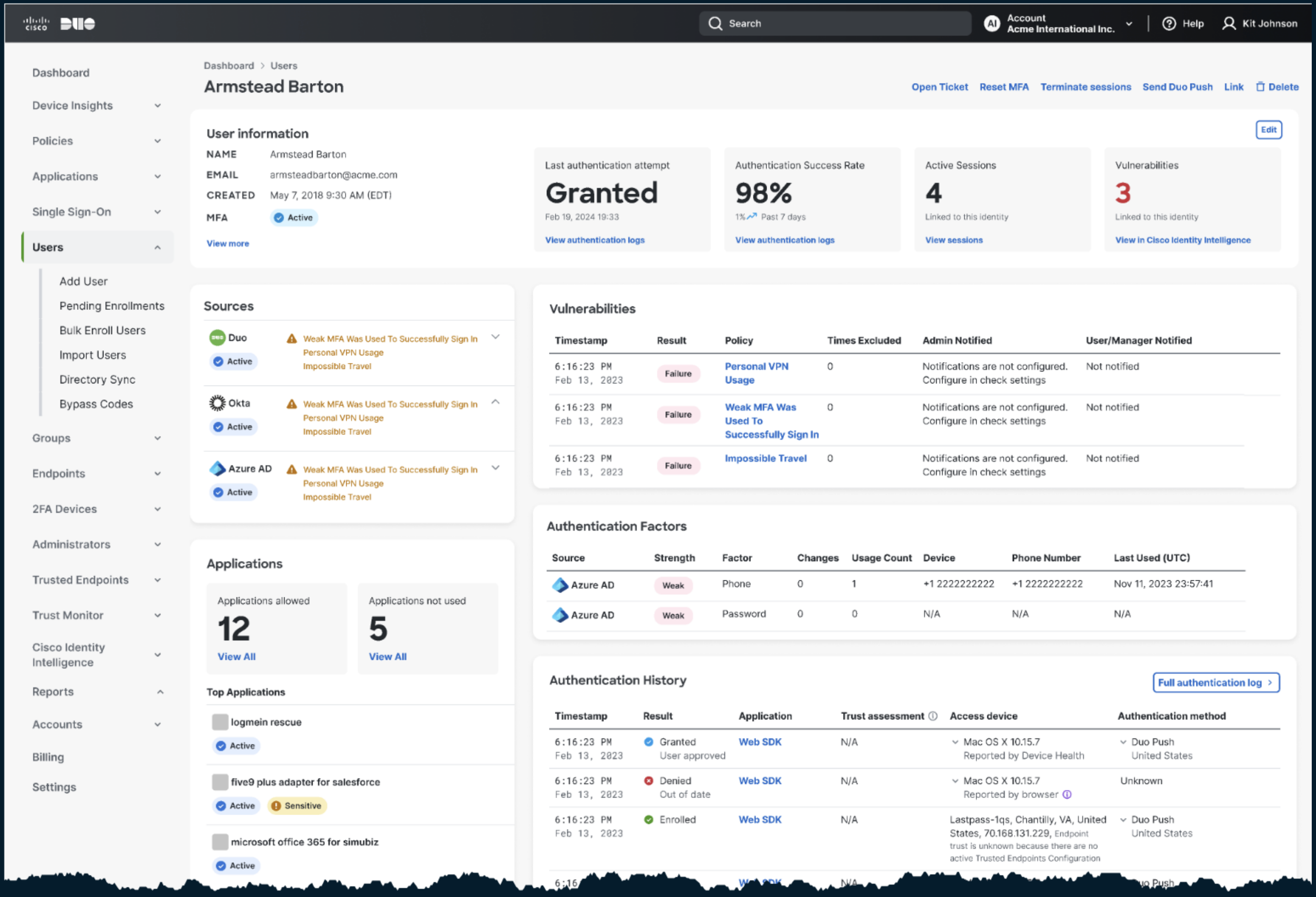
Duo Integration Details

- Three Duo API's in use:
  - Admin API
  - Auth API
  - Streaming API (new, non-public)
    - If you do not use the Identity Intelligence Wizard, a TAC case is required to enable streaming (for now)
- Identity Intelligence
  - Management API (non-public)
  - Public API
  - Webhook notifications



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!



Dashboard > Users

Armstead Barton

User information

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

View more

Last authentication attempt
Granted
Feb 19, 2024 19:33
View authentication logs

Authentication Success Rate
98%
1% Past 7 days
View authentication logs

Active Sessions
4
Linked to this identity
View sessions

Vulnerabilities
3
Linked to this identity
View in Cisco Identity Intelligence

Sources

Duo Active	Weak MFA Was Used To Successfully Sign In Personal VPN Usage Impossible Travel
Okta Active	Weak MFA Was Used To Successfully Sign In Personal VPN Usage Impossible Travel
Azure AD Active	Weak MFA Was Used To Successfully Sign In Personal VPN Usage Impossible Travel

Vulnerabilities

Timestamp	Result	Policy	Times Excluded	Admin Notified	User/Manager Notified
6:16:23 PM Feb 13, 2023	Failure	Personal VPN Usage	0	Notifications are not configured. Configure in check settings	Not notified
6:16:23 PM Feb 13, 2023	Failure	Weak MFA Was Used To Successfully Sign In	0	Notifications are not configured. Configure in check settings	Not notified
6:16:23 PM Feb 13, 2023	Failure	Impossible Travel	0	Notifications are not configured. Configure in check settings	Not notified

Applications

Applications allowed
12
View All

Applications not used
5
View All

Top Applications

- logmein rescue — Active
- five9 plus adapter for salesforce — Active, Sensitive
- microsoft office 365 for simubiz — Active

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

Full authentication log >

Timestamp	Result	Application	Trust assessment	Access device	Authentication method
6:16:23 PM Feb 13, 2023	Granted User approved	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 Out of date	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, 70.168.131.229, Endpoint trust is unknown because there are no active Trusted Endpoints Configuration	Duo Push United States

cisco Live!

Cisco XDR
Splunk SOAR
etc.

Trick of the Trade

Webhooks w/ Cisco XDR

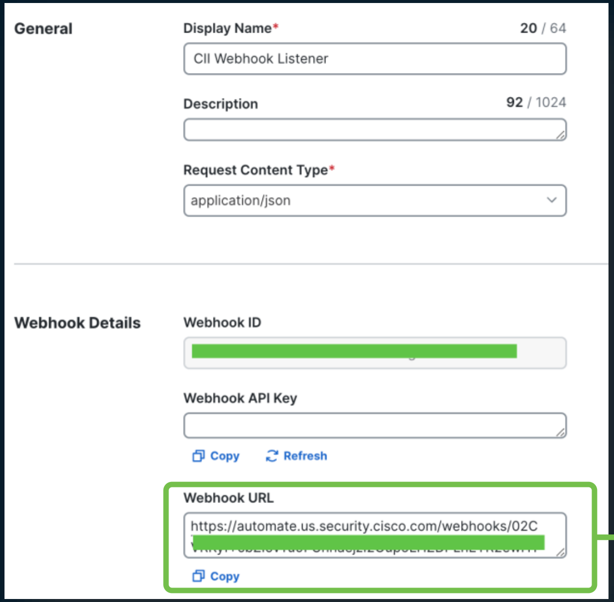
Webhook URL

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



General

Display Name* 20 / 64

CII Webhook Listener

Description 92 / 1024

Request Content Type*

application/json

Webhook Details

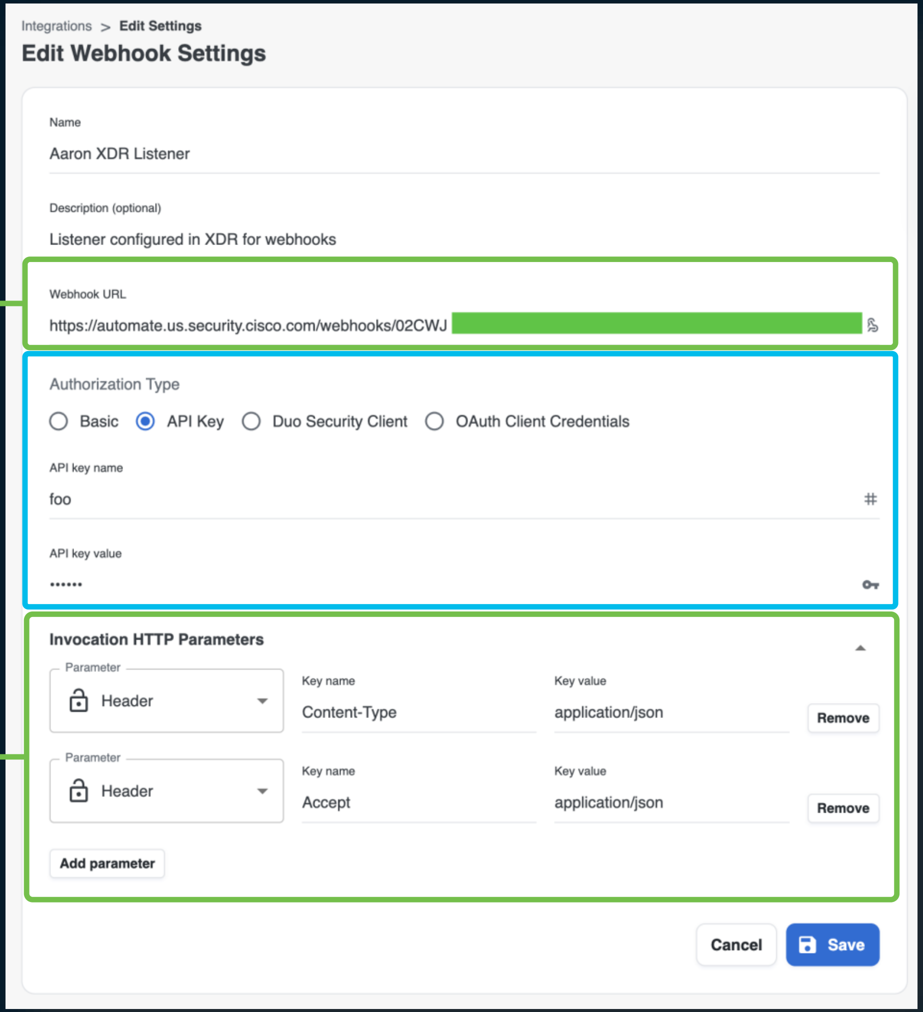
Webhook ID

[redacted]

Webhook API Key

Webhook URL

https://automate.us.security.cisco.com/webhooks/02C [redacted]



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 [redacted]

Authorization Type

○ Basic ● API Key ○ Duo Security Client ○ OAuth Client Credentials

API key name

foo

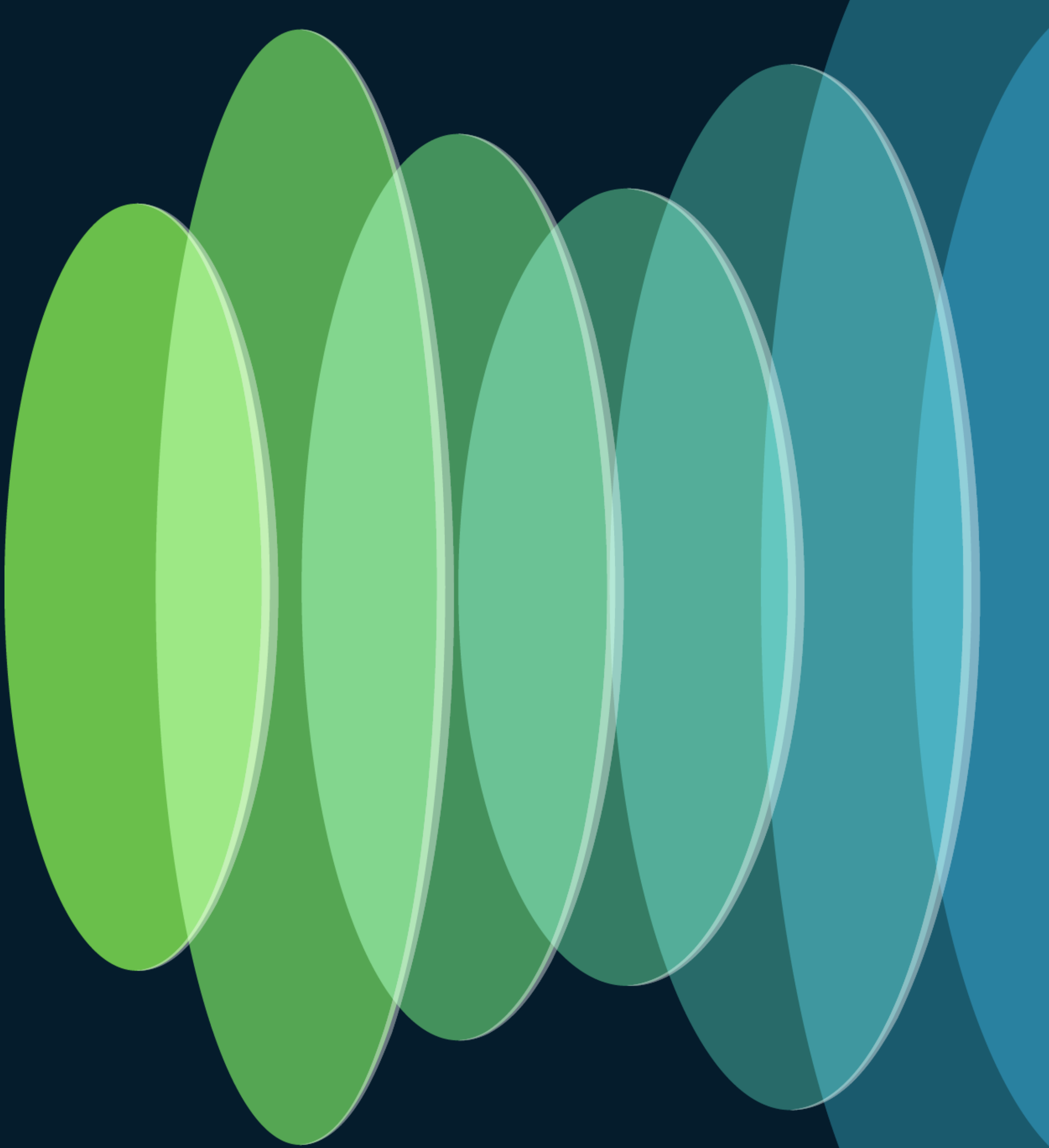
API key value

••••••

Invocation HTTP Parameters

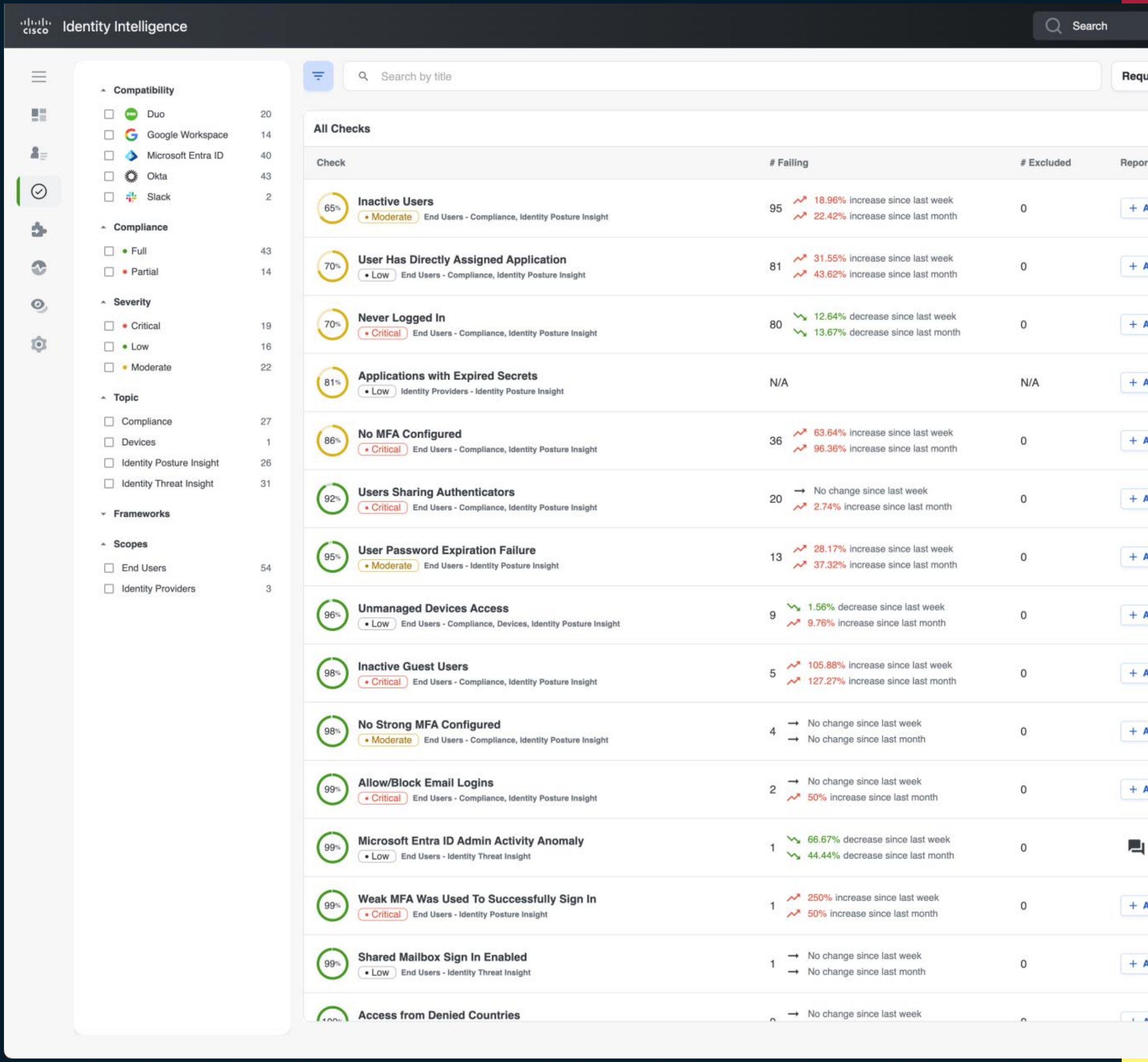
Parameter	Key name	Key value	
Header	Content-Type	application/json	Remove
Header	Accept	application/json	Remove

All about those Checks



What are Checks?

- These are like “signatures” in an IDS
- When the collected data matches a check… That check is recorded as failed.



Identity Intelligence

Search

Search by title

Requ

Compatibility

□	Duo	20
□	Google Workspace	14
□	Microsoft Entra ID	40
□	Okta	43
□	Slack	2

Compliance

□	● Full	43
□	● Partial	14

Severity

□	● Critical	19
□	● Low	16
□	● Moderate	22

Topic

□	Compliance	27
□	Devices	1
□	Identity Posture Insight	26
□	Identity Threat Insight	31

Frameworks

Scopes

□	End Users	54
□	Identity Providers	3

All Checks

Check	# Failing		# Excluded	Repor
65% Inactive Users ● Moderate End Users - Compliance, Identity Posture Insight	95	18.96% increase since last week 22.42% increase since last month	0	+ A
70% 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	+ A
70% Never Logged In ● Critical End Users - Compliance, Identity Posture Insight	80	12.64% decrease since last week 13.67% decrease since last month	0	+ A
81% Applications with Expired Secrets ● Low Identity Providers - Identity Posture Insight	N/A		N/A	+ A
86% No MFA Configured ● Critical End Users - Compliance, Identity Posture Insight	36	63.64% increase since last week 96.36% increase since last month	0	+ A
92% Users Sharing Authenticators ● Critical End Users - Compliance, Identity Posture Insight	20	→ No change since last week 2.74% increase since last month	0	+ A
95% User Password Expiration Failure ● Moderate End Users - Identity Posture Insight	13	28.17% increase since last week 37.32% increase since last month	0	+ A
96% 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	+ A
98% Inactive Guest Users ● Critical End Users - Compliance, Identity Posture Insight	5	105.88% increase since last week 127.27% increase since last month	0	+ A
98% No Strong MFA Configured ● Moderate End Users - Compliance, Identity Posture Insight	4	→ No change since last week → No change since last month	0	+ A
99% Allow/Block Email Logins ● Critical End Users - Compliance, Identity Posture Insight	2	→ No change since last week 50% increase since last month	0	+ A
99% 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	
99% 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	+ A
99% Shared Mailbox Sign In Enabled ● Low End Users - Identity Threat Insight	1	→ No change since last week → No change since last month	0	+ A
Access from Denied Countries	[illegible]	→ No change since last week	[illegible]	

Compatibility

Not all checks are compatible with all providers / sources.

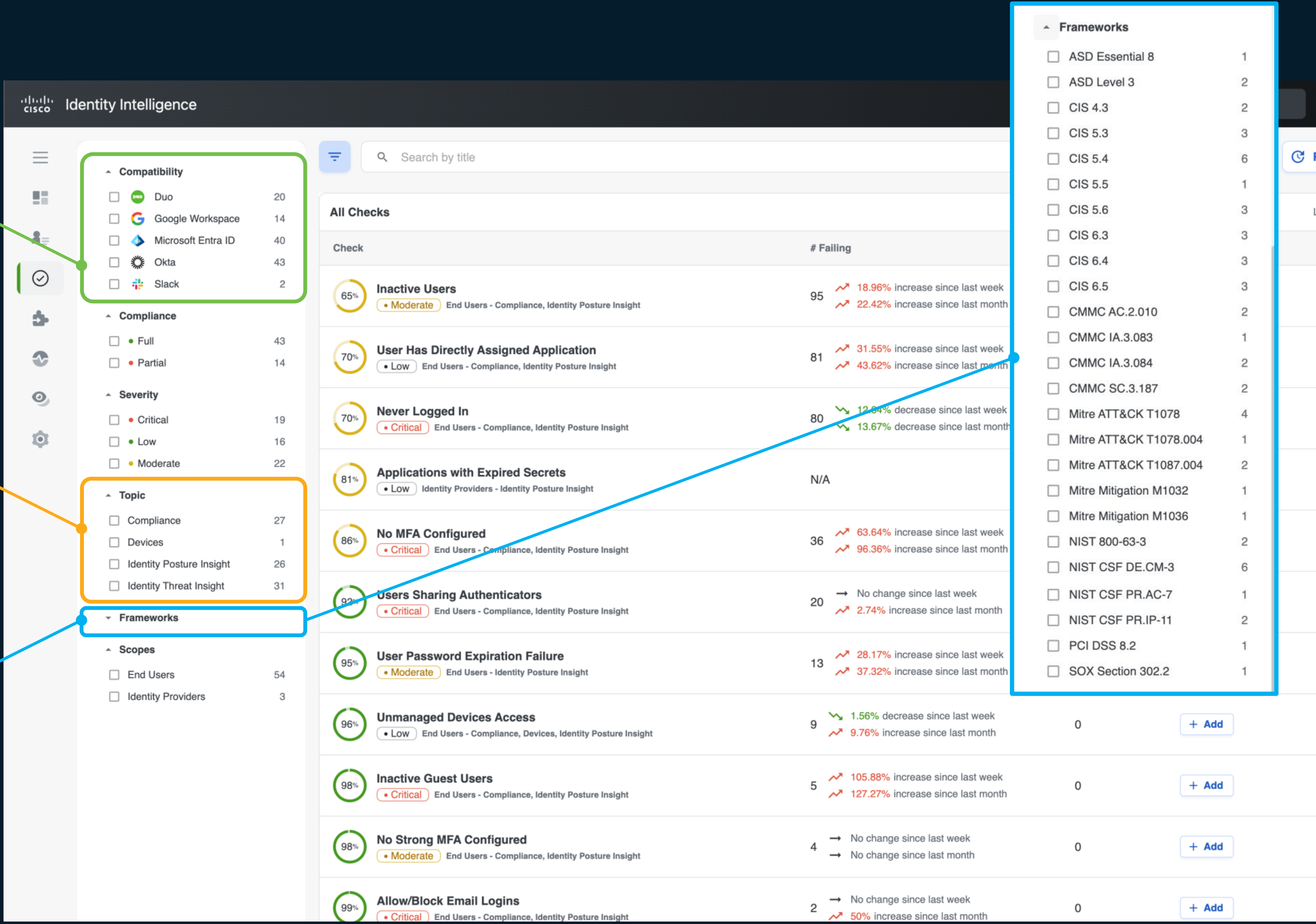
You can filter the list of checks based on the IdP source

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.



Compatibility

□ Duo	20
□ Google Workspace	14
□ Microsoft Entra ID	40
□ Okta	43
□ Slack	2

Compliance

□ ● Full	43
□ ● Partial	14

Severity

□ ● Critical	19
□ ● Low	16
□ ● Moderate	22

Topic

□ Compliance	27
□ Devices	1
□ Identity Posture Insight	26
□ Identity Threat Insight	31

Frameworks

Scopes

□ End Users	54
□ Identity Providers	3

All Checks

Check	# Failing			
65% Inactive Users ● Moderate End Users - Compliance, Identity Posture Insight	95	18.96% increase since last week 22.42% increase since last month		
70% 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		
70% Never Logged In ● Critical End Users - Compliance, Identity Posture Insight	80	12.64% decrease since last week 13.67% decrease since last month		
81% Applications with Expired Secrets ● Low Identity Providers - Identity Posture Insight	N/A			
86% No MFA Configured ● Critical End Users - Compliance, Identity Posture Insight	36	63.64% increase since last week 96.36% increase since last month		
92% Users Sharing Authenticators ● Critical End Users - Compliance, Identity Posture Insight	20	No change since last week 2.74% increase since last month		
95% User Password Expiration Failure ● Moderate End Users - Identity Posture Insight	13	28.17% increase since last week 37.32% increase since last month		
96% 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	+ Add
98% Inactive Guest Users ● Critical End Users - Compliance, Identity Posture Insight	5	105.88% increase since last week 127.27% increase since last month	0	+ Add
98% No Strong MFA Configured ● Moderate End Users - Compliance, Identity Posture Insight	4	No change since last week No change since last month	0	+ Add
99% Allow/Block Email Logins ● Critical End Users - Compliance, Identity Posture Insight	2	No change since last week 50% increase since last month	0	+ Add

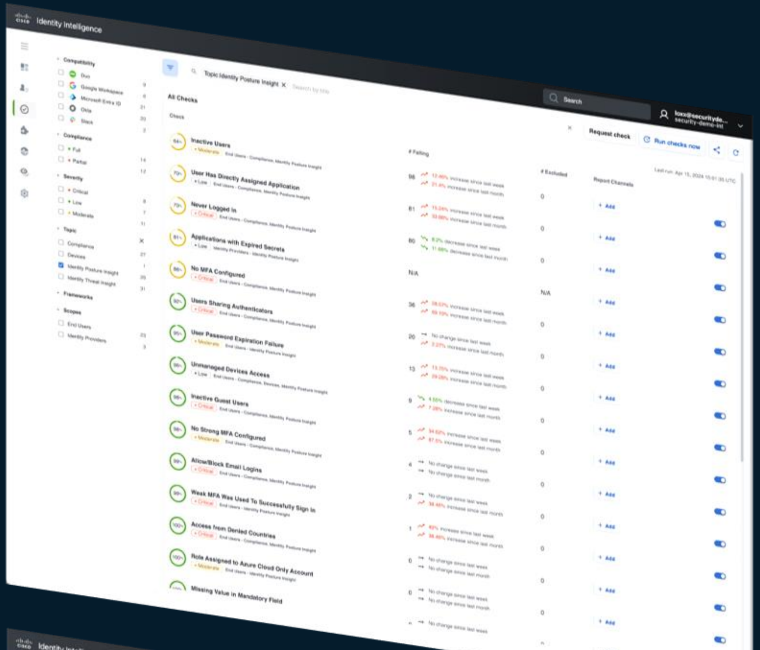
Frameworks

□ ASD Essential 8	1
□ ASD Level 3	2
□ CIS 4.3	2
□ CIS 5.3	3
□ CIS 5.4	6
□ CIS 5.5	1
□ CIS 5.6	3
□ CIS 6.3	3
□ CIS 6.4	3
□ CIS 6.5	3
□ CMMC AC.2.010	2
□ CMMC IA.3.083	1
□ CMMC IA.3.084	2
□ CMMC SC.3.187	2
□ Mitre ATT&CK T1078	4
□ Mitre ATT&CK T1078.004	1
□ Mitre ATT&CK T1087.004	2
□ Mitre Mitigation M1032	1
□ Mitre Mitigation M1036	1
□ NIST 800-63-3	2
□ NIST CSF DE.CM-3	6
□ NIST CSF PR.AC-7	1
□ NIST CSF PR.IP-11	2
□ PCI DSS 8.2	1
□ SOX Section 302.2	1

Proactive vs. Reactive

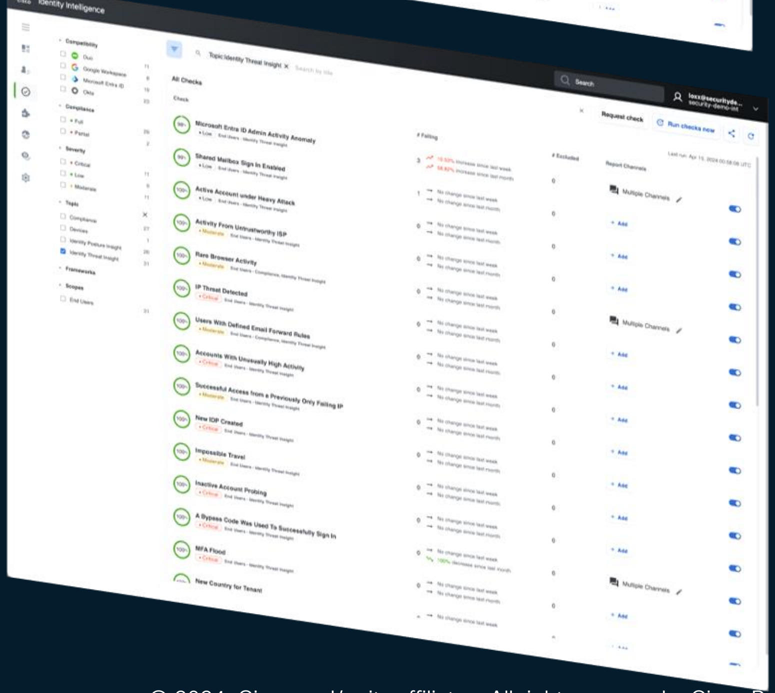
- Posture Checks are Proactive – examining the authentications and account configurations – to reduce probability and blast radius

- Threat Checks are Reactive – examining the behavior of users and their authentications – to detect threats



All Checks

Check		# Failing	# Excluded
Inactive Users	Moderate	98	0
User Has Directly Assigned Application	Low	81	0
Never Logged In	Critical	80	0
Applications with Expired Secrets	Low	N/A	N/A
No MFA Configured	Critical	36	0
Users Sharing Authenticators	Critical	20	0
User Password Expiration Failure	Moderate	13	0
Unmanaged Devices Access	Low	9	0
Inactive Guest Users	Critical	5	0
No Strong MFA Configured	Moderate	4	0
Allow/Block Email Logins	Critical	2	0
Weak MFA Was Used To Successfully Sign In	Critical	1	0
Access from Denied Countries	Critical	0	0
Role Assigned to Azure Cloud Only Account	Moderate	0	0
Missing Value in Mandatory Field		–	

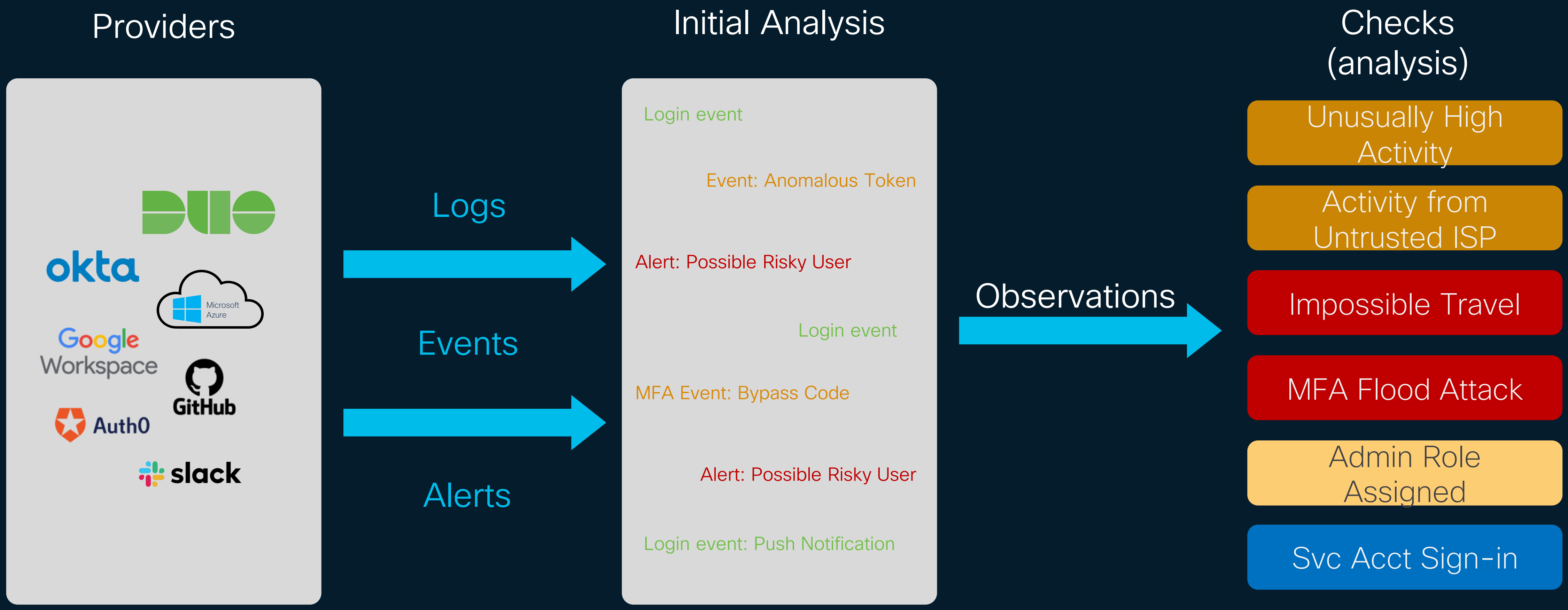


All Checks

Check		# Failing	# Excluded
Microsoft Entra ID Admin Activity Anomaly	Low	3	0
Shared Mailbox Sign In Enabled	Low	1	0
Active Account under Heavy Attack	Low	0	0
Activity From Untrustworthy ISP	Moderate	0	0
Rare Browser Activity	Moderate	0	0
IP Threat Detected	Critical	0	0
Users With Defined Email Forward Rules	Moderate	0	0
Accounts With Unusually High Activity	Critical	0	0
Successful Access from a Previously Only Failing IP	Moderate	0	0
New IDP Created	Critical	0	0
Impossible Travel	Moderate	0	0
Inactive Account Probing	Critical	0	0
A Bypass Code Was Used To Successfully Sign In	Critical	0	0
MFA Flood	Critical	0	0
New Country for Tenant		–	

Observations and Checks

- Threat Detection signatures can use Observations.
- Posture (ISPM) Checks do not use observations, those are direct.



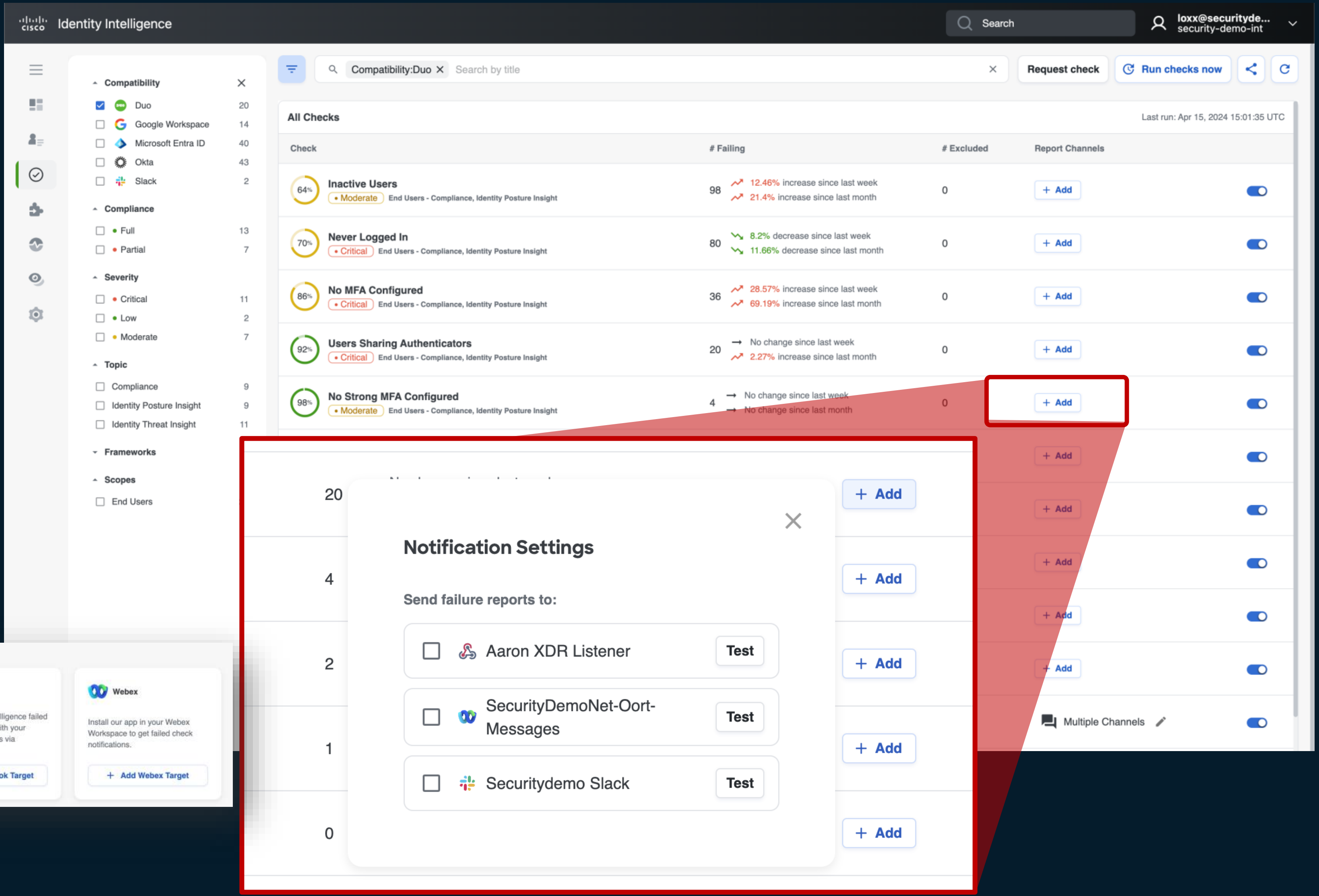
Notifications when a check is matched

Notifications

Notifications are configured per check.

Checks are run periodically, matching the data in the CII 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.



Identity Intelligence

Search

loxx@securityde... security-demo-int

Compatibility

- ☑ Duo 20
- ☐ Google Workspace 14
- ☐ Microsoft Entra ID 40
- ☐ Okta 43
- ☐ Slack 2

Compliance

- ☐ ● Full 13
- ☐ ● Partial 7

Severity

- ☐ ● Critical 11
- ☐ ● Low 2
- ☐ ● Moderate 7

Topic

- ☐ Compliance 9
- ☐ Identity Posture Insight 9
- ☐ Identity Threat Insight 11

Frameworks

Scopes

- ☐ End Users

Compatibility:Duo ✕ Search by title

Request check | Run checks now

All Checks — Last run: Apr 15, 2024 15:01:35 UTC

Check	# Failing		# Excluded	Report Channels
64% Inactive Users • Moderate End Users - Compliance, Identity Posture Insight	98	12.46% increase since last week 21.4% increase since last month	0	+ Add
70% Never Logged In • Critical End Users - Compliance, Identity Posture Insight	80	8.2% decrease since last week 11.66% decrease since last month	0	+ Add
86% No MFA Configured • Critical End Users - Compliance, Identity Posture Insight	36	28.57% increase since last week 69.19% increase since last month	0	+ Add
92% Users Sharing Authenticators • Critical End Users - Compliance, Identity Posture Insight	20	No change since last week 2.27% increase since last month	0	+ Add
98% No Strong MFA Configured • Moderate End Users - Compliance, Identity Posture Insight	4	No change since last week No change since last month	0	+ Add

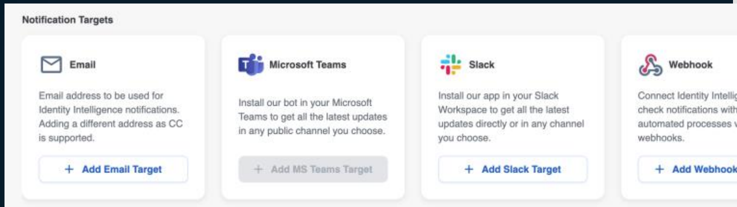
Multiple Channels

Notification Settings

Send failure reports to:

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

Notifications Targets:



Notification Targets

Email

Email address to be used for Identity Intelligence notifications. Adding a different address as CC is supported.

+ Add Email Target

Microsoft Teams

Install our bot in your Microsoft Teams to get all the latest updates in any public channel you choose.

+ Add MS Teams Target

Slack

Install our app in your Slack Workspace to get all the latest updates directly or in any channel you choose.

+ Add Slack Target

Webhook

Connect Identity Intelligence failed check notifications with your automated processes via webhooks.

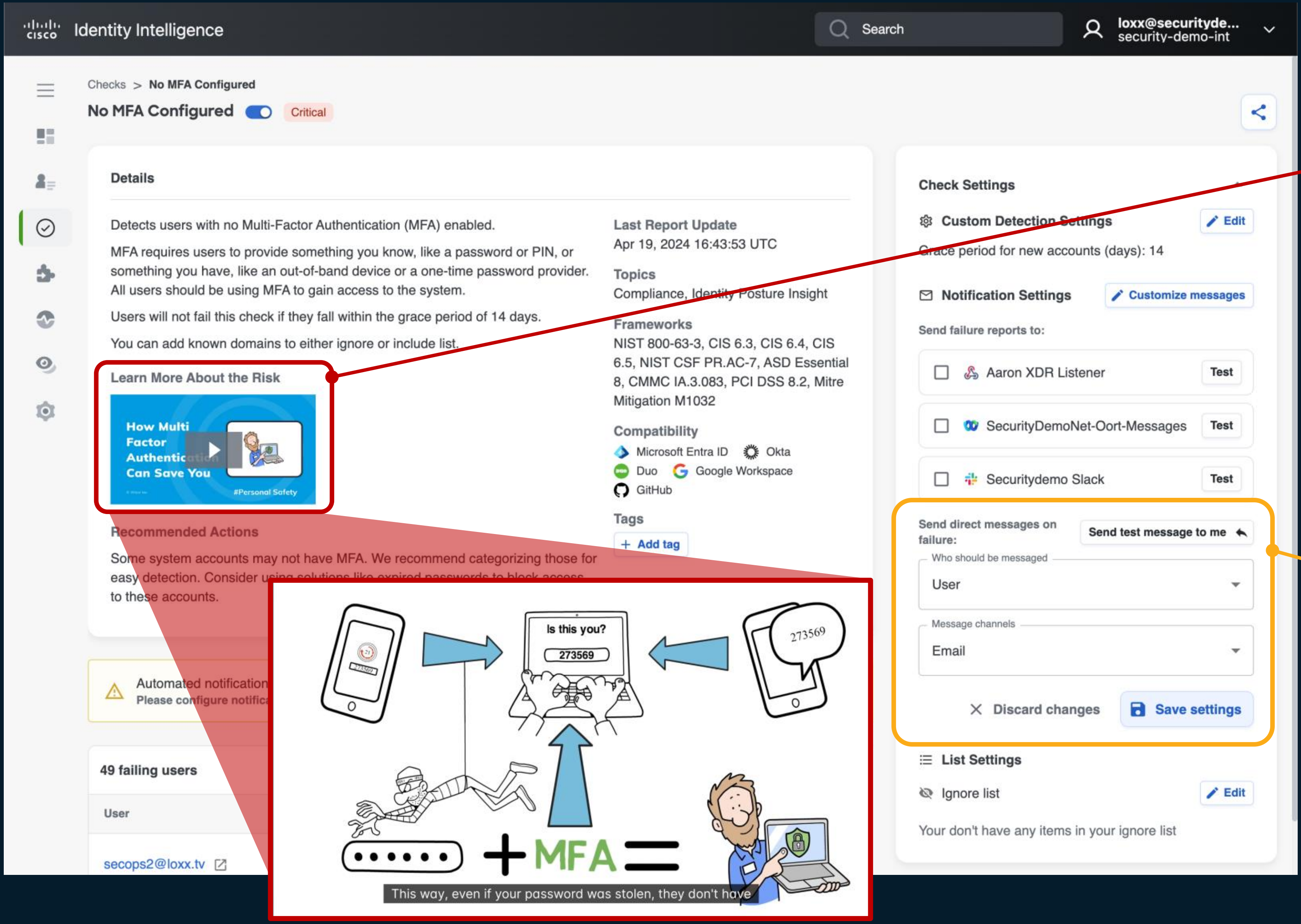
+ Add Webhook Target

Webex

Install our app in your Webex Workspace to get failed check notifications.

+ Add Webex Target

Notifications when a check is matched



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.

Last Report Update
Apr 19, 2024 16:43:53 UTC

Topics
Compliance, Identity Posture Insight

Frameworks
NIST 800-63-3, CIS 6.3, CIS 6.4, CIS 6.5, NIST CSF PR.AC-7, ASD Essential 8, CMMC IA.3.083, PCI DSS 8.2, Mitre Mitigation M1032

Compatibility
Microsoft Entra ID, Okta, Duo, Google Workspace, GitHub

Tags
+ Add tag

Learn More About the Risk

Recommended Actions

Some system accounts may not have MFA. We recommend categorizing those for easy detection. Consider using solutions like expired passwords to block access to these accounts.

Automated notification
Please configure notific

49 failing users

User

secops2@loxx.tv

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: Send test message to me

Who should be messaged: User

Message channels: Email

Discard changes — Save settings

List Settings

Ignore list — Edit

Your don't have any items in your ignore list

Security Education

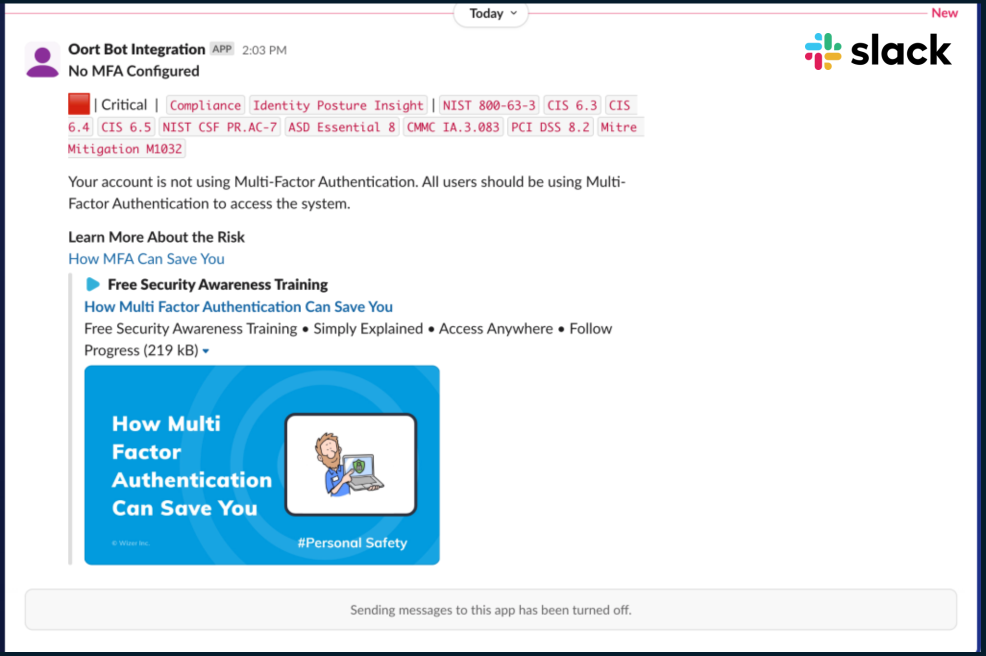
CII partners with Wizer (https://www.wizer-training.com/) and their very cool security education videos to help educate the end-user on what they did wrong & why it matters.

Educate the End-User

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

cisco Live!

Notifications when a check is matched



Today · New

Oort Bot Integration APP 2:03 PM

No MFA Configured

🟥 | Critical | `Compliance` `Identity Posture Insight` | `NIST 800-63-3` `CIS 6.3` `CIS 6.4` `CIS 6.5` `NIST CSF PR.AC-7` `ASD Essential 8` `CMMC IA.3.083` `PCI DSS 8.2` `Mitre Mitigation M1032`

Your account is not using Multi-Factor Authentication. All users should be using Multi-Factor Authentication to access the system.

Learn More About the Risk

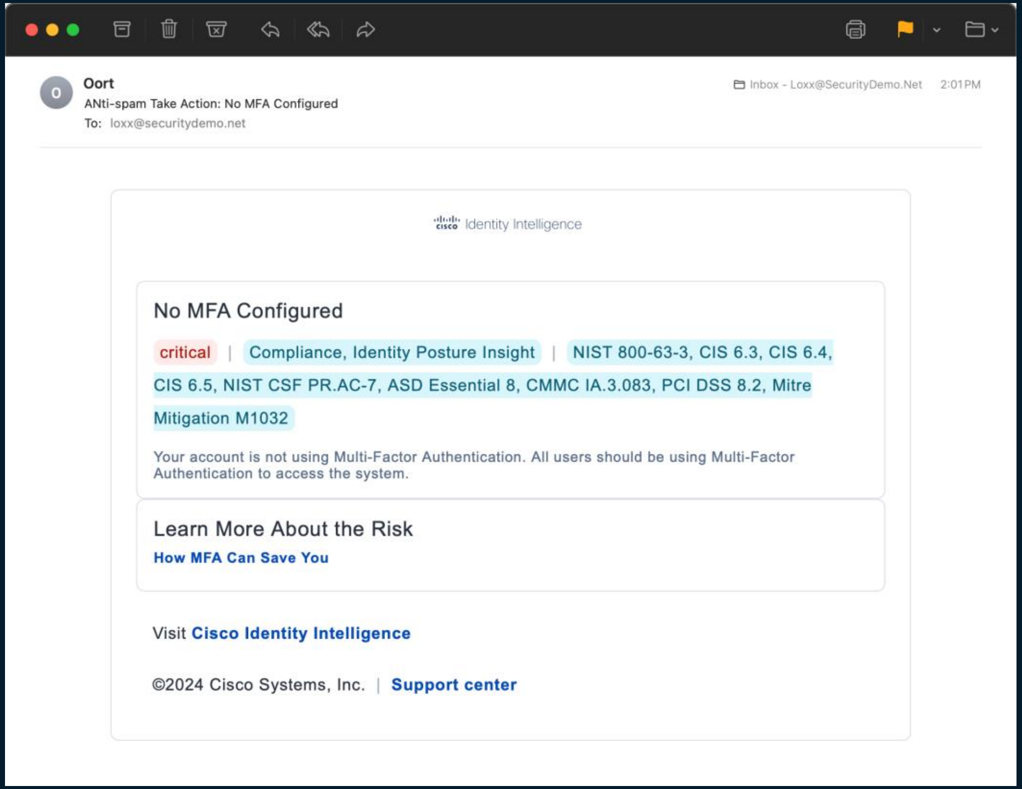
How MFA Can Save You

Free Security Awareness Training

How Multi Factor Authentication Can Save You

Free Security Awareness Training • Simply Explained • Access Anywhere • Follow Progress (219 kB)

Sending messages to this app has been turned off.



Oort

ANti-spam Take Action: No MFA Configured

To: loxx@securitydemo.net

Inbox - Loxx@SecurityDemo.Net 2:01PM

Identity Intelligence

No MFA Configured

critical | Compliance, Identity Posture Insight | NIST 800-63-3, CIS 6.3, CIS 6.4, CIS 6.5, NIST CSF PR.AC-7, ASD Essential 8, CMMC IA.3.083, PCI DSS 8.2, Mitre Mitigation M1032

Your account is not using Multi-Factor Authentication. All users should be using Multi-Factor Authentication to access the system.

Learn More About the Risk

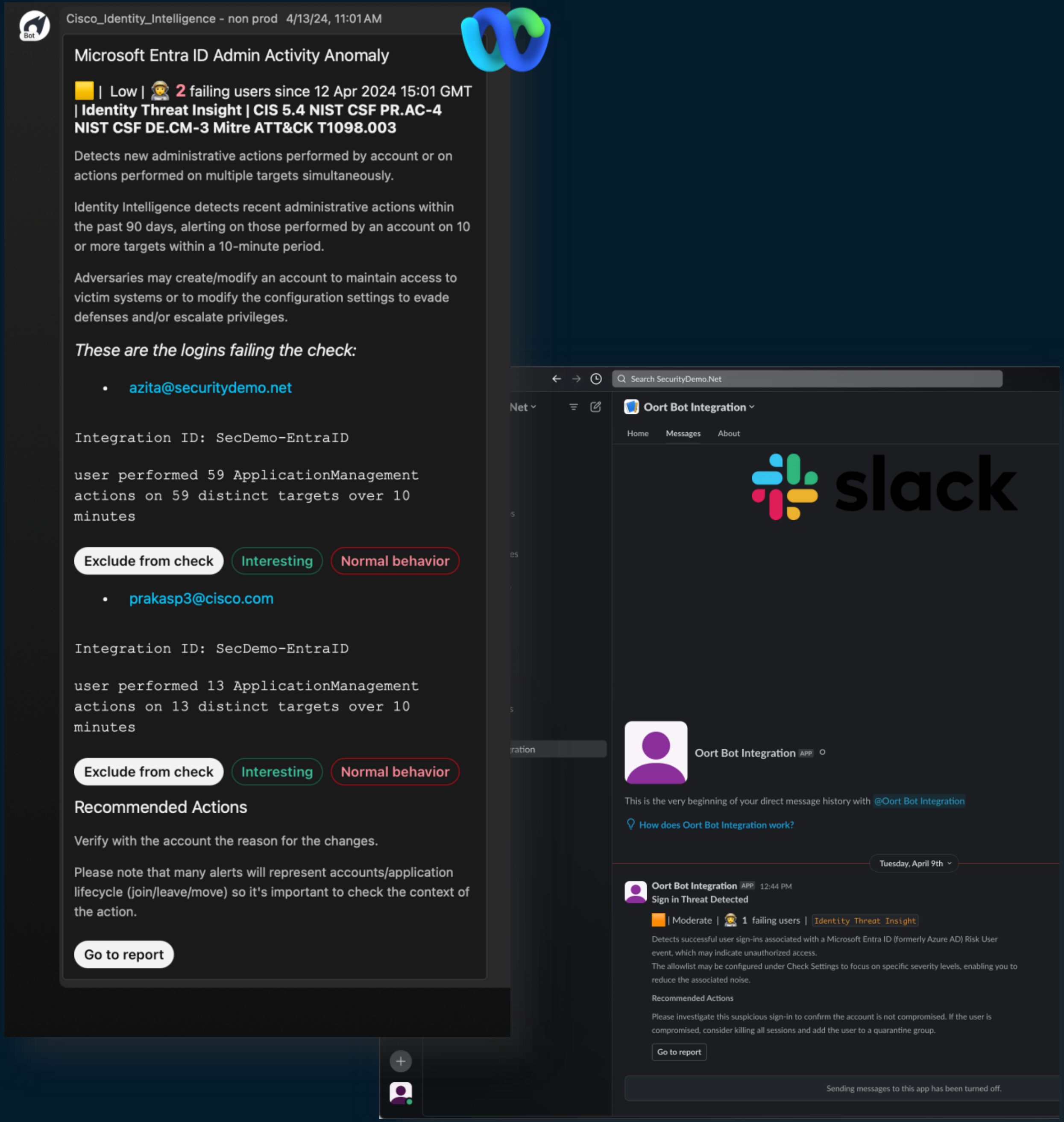
How MFA Can Save You

Visit **Cisco Identity Intelligence**

©2024 Cisco Systems, Inc. | **Support center**

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



Cisco_Identity_Intelligence - non prod 4/13/24, 11:01 AM

Microsoft Entra ID Admin Activity Anomaly

🟨 | Low | 🧑‍🚀 2 failing users since 12 Apr 2024 15:01 GMT | **Identity Threat Insight | CIS 5.4 NIST CSF PR.AC-4 NIST CSF DE.CM-3 Mitre ATT&CK T1098.003**

Detects new administrative actions performed by account or on actions performed on multiple targets simultaneously.

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.

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.

These are the logins failing the check:

- azita@securitydemo.net

```
Integration ID: SecDemo-EntraID

user performed 59 ApplicationManagement
actions on 59 distinct targets over 10
minutes
```

Exclude from check | Interesting | Normal behavior

- prakasp3@cisco.com

```
Integration ID: SecDemo-EntraID

user performed 13 ApplicationManagement
actions on 13 distinct targets over 10
minutes
```

Exclude from check | Interesting | Normal behavior

Recommended Actions

Verify with the account the reason for the changes.

Please note that many alerts will represent accounts/application lifecycle (join/leave/move) so it's important to check the context of the action.

Go to report

Oort Bot Integration APP

This is the very beginning of your direct message history with @Oort Bot Integration

How does Oort Bot Integration work?

Tuesday, April 9th

Oort Bot Integration APP 12:44 PM

Sign in Threat Detected

🟧 | Moderate | 🧑‍🚀 1 failing users | `Identity Threat Insight`

Detects successful user sign-ins associated with a Microsoft Entra ID (formerly Azure AD) Risk User event, which may indicate unauthorized access.

The allowlist may be configured under Check Settings to focus on specific severity levels, enabling you to reduce the associated noise.

Recommended Actions

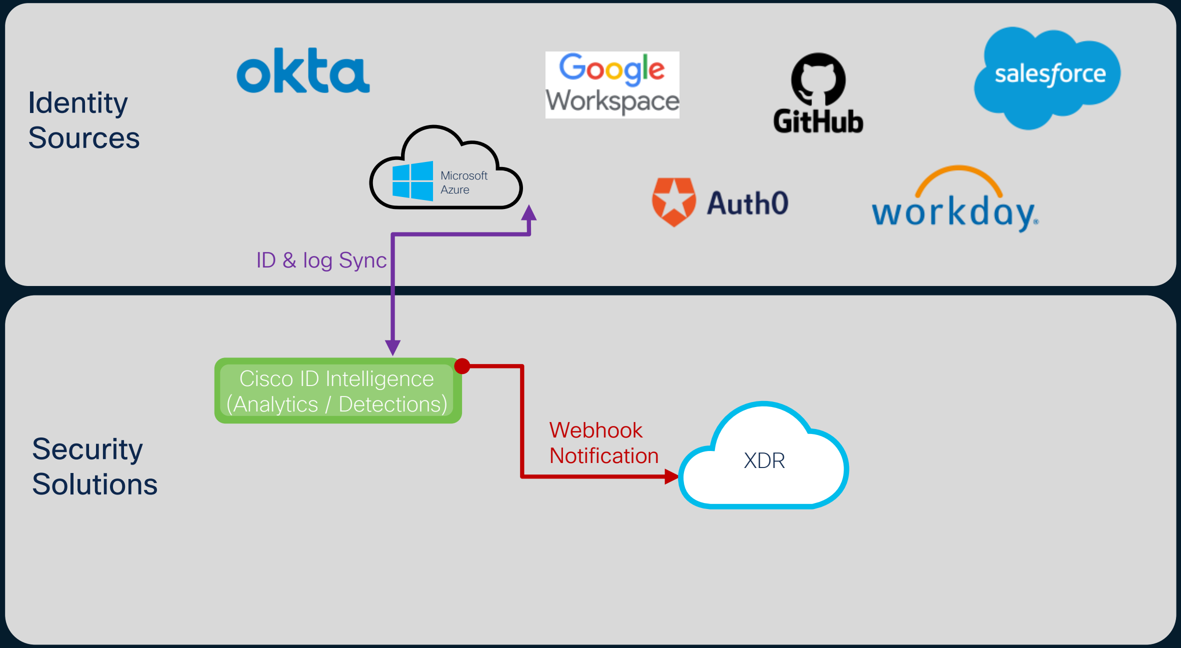
Please investigate this suspicious sign-in to confirm the account is not compromised. If the user is compromised, consider killing all sessions and add the user to a quarantine group.

Go to report

Sending messages to this app has been turned off.

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



Checks are Tunable

Check Settings

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

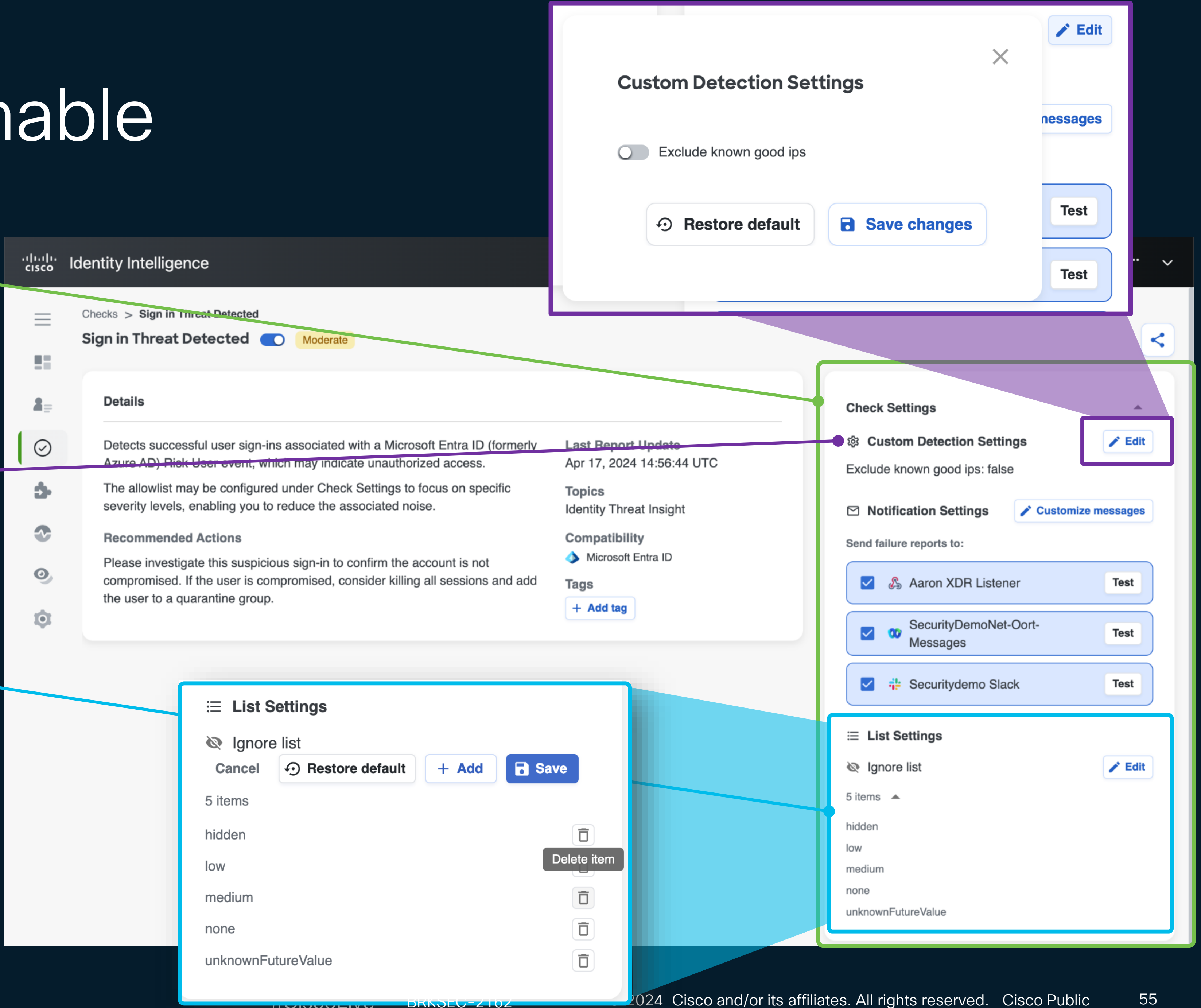
Custom Detection Settings

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



Custom Detection Settings

Exclude known good ips

Identity Intelligence

Checks > Sign in Threat Detected

Sign in Threat Detected — Moderate

Details

Detects successful user sign-ins associated with a Microsoft Entra ID (formerly Azure AD) Risk User event, which may indicate unauthorized access.

The allowlist may be configured under Check Settings to focus on specific severity levels, enabling you to reduce the associated noise.

Recommended Actions

Please investigate this suspicious sign-in to confirm the account is not compromised. If the user is compromised, consider killing all sessions and add the user to a quarantine group.

Last Report Update: Apr 17, 2024 14:56:44 UTC

Topics: Identity Threat Insight

Compatibility: Microsoft Entra ID

Tags

Check Settings

Custom Detection Settings

Exclude known good ips: false

Notification Settings

Send failure reports to:

- ☑ Aaron XDR Listener
- ☑ SecurityDemoNet-Oort-Messages
- ☑ Securitydemo Slack

List Settings

Ignore list

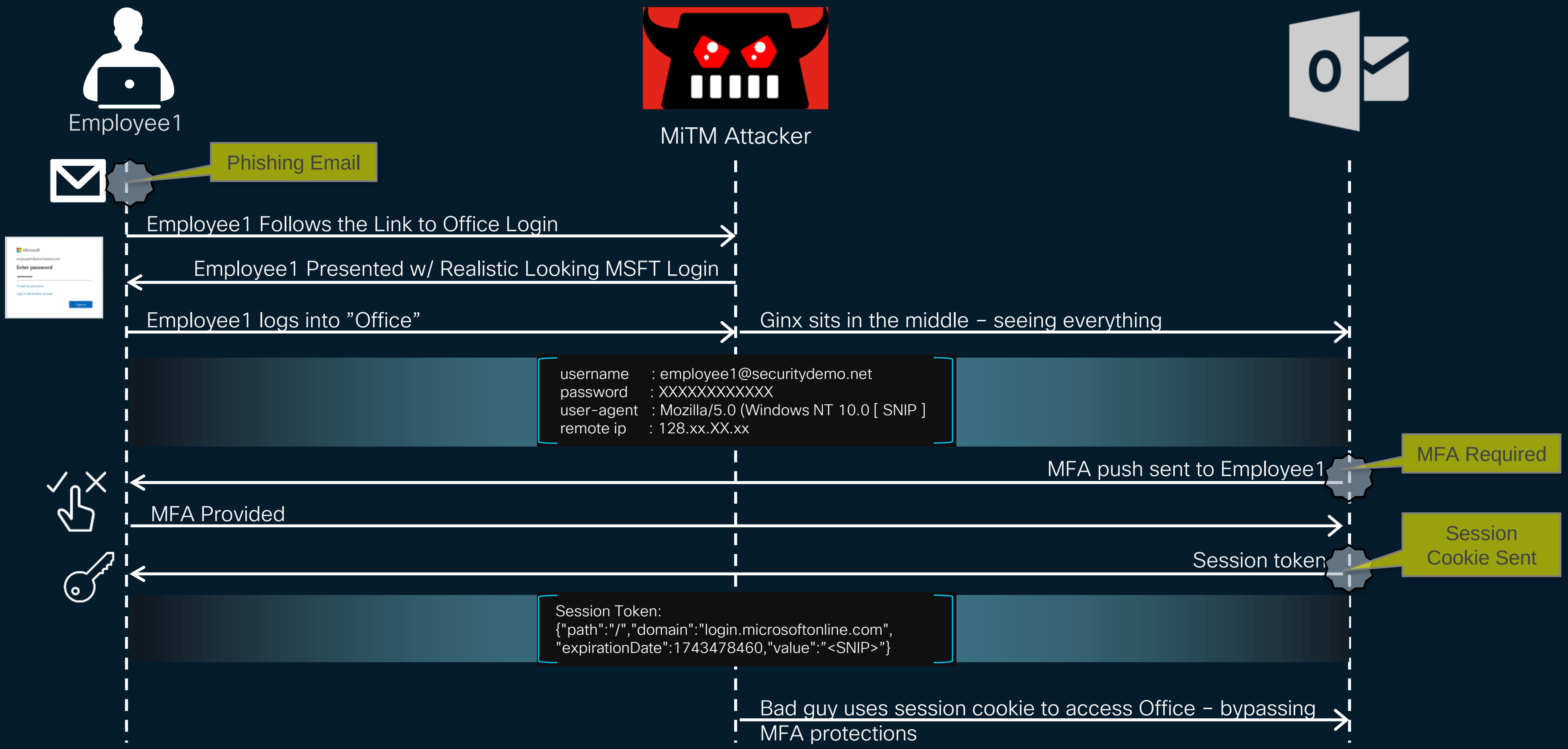
5 items

- hidden
- low
- medium
- none
- unknownFutureValue

Session Hijacking Example

Session Hijacks are on the rise

- Can be accomplished with a machine-in-the-middle
  - Including malware that is installed on the endpoint
  - The bad-actor collects the session data from the victim
  - Uses the same session keys (Auth, or even Re-Auth tokens)
- These can be signed to last for hours, days, weeks or even longer!
  - The way “Modern Auth” (aka: WebAuth with SAML or OAuth/OIDC) works
  - The authenticating app (service provider) checks the validity of the bearer-token being signed by a trusted IdP w/ a valid lifetime > then issues the session cookie
  - The SP doesn’t check back with the IdP until the session expires!



Employee1

MiTM Attacker

Phishing Email

Employee1 Follows the Link to Office Login

Employee1 Presented w/ Realistic Looking MSFT Login

Employee1 logs into ”Office”

Ginx sits in the middle – seeing everything

```
username    : employee1@securitydemo.net
password    : XXXXXXXXXXXX
user-agent  : Mozilla/5.0 (Windows NT 10.0 [ SNIP ]
remote ip   : 128.xx.XX.xx
```

MFA Required

MFA push sent to Employee1

MFA Provided

Session Cookie Sent

Session token

```
Session Token:
{"path":"/","domain":"login.microsoftonline.com",
"expirationDate":1743478460,"value":”<SNIP>”}
```

Bad guy uses session cookie to access Office – bypassing MFA protections

What the Bad Actor sees

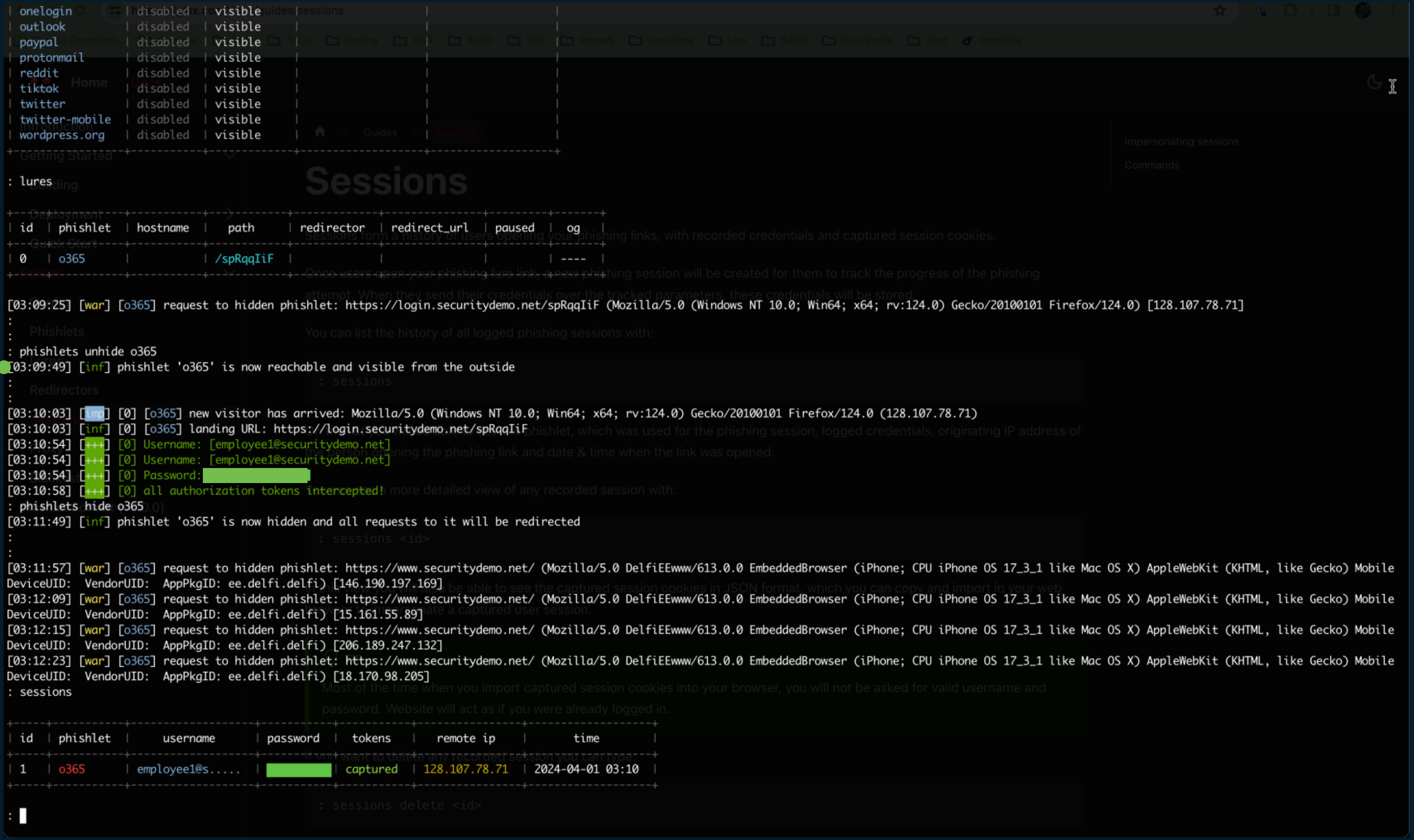
Lure them in

Usually starts with a phishing attack (still #1 vector)

User follows the link & sees what looks exactly like the normal Microsoft Login flow

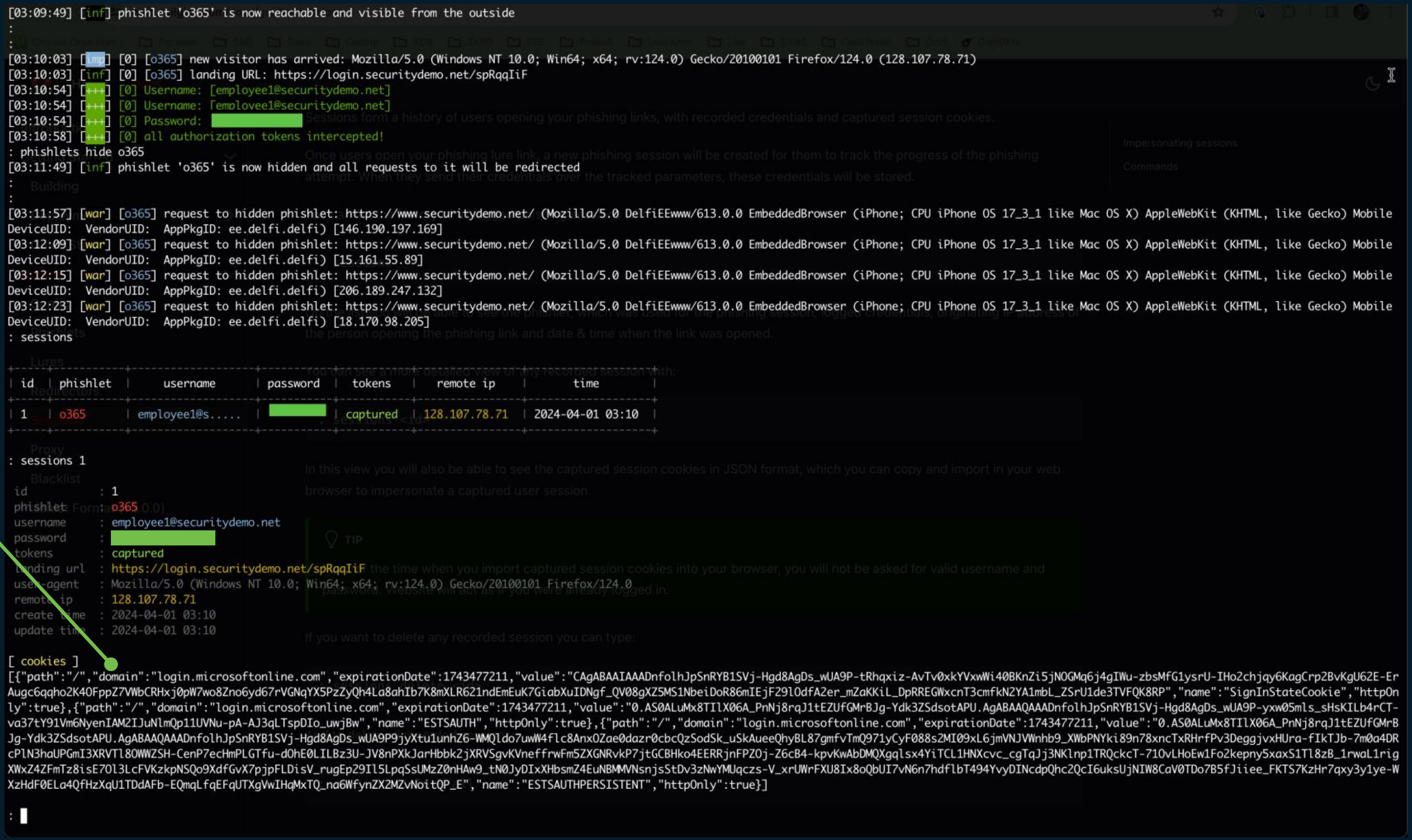
Bad Guy sees everything

The bad guy is able to capture the username, password (most times) & more importantly the Session Info, including the cookie



```
| onelogin       | disabled | visible |               |               |
| outlook        | disabled | visible |               |               |
| paypal         | disabled | visible |               |               |
| protonmail     | disabled | visible |               |               |
| reddit         | disabled | visible |               |               |
| tiktok         | disabled | visible |               |               |
| twitter        | disabled | visible |               |               |
| twitter-mobile | disabled | visible |               |               |
| wordpress.org  | disabled | visible |               |               |
+----------------+----------+---------+---------------+---------------+

: lures

+----+----------+----------+-----------+------------+--------------+--------+------+
| id | phishlet | hostname |   path    | redirector | redirect_url | paused |  og  |
+----+----------+----------+-----------+------------+--------------+--------+------+
| 0  | o365     |          | /spRqqIiF |            |              |        | ---- |
+----+----------+----------+-----------+------------+--------------+--------+------+

[03:09:25] [war] [o365] request to hidden phishlet: https://login.securitydemo.net/spRqqIiF (Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0) [128.107.78.71]
:
:
: phishlets unhide o365
[03:09:49] [inf] phishlet 'o365' is now reachable and visible from the outside
:
:
[03:10:03] [imp] [0] [o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0 (128.107.78.71)
[03:10:03] [inf] [0] [o365] landing URL: https://login.securitydemo.net/spRqqIiF
[03:10:54] [+++] [0] Username: [employee1@securitydemo.net]
[03:10:54] [+++] [0] Username: [employee1@securitydemo.net]
[03:10:54] [+++] [0] Password: [redacted]
[03:10:58] [+++] [0] all authorization tokens intercepted!
: phishlets hide o365
[03:11:49] [inf] phishlet 'o365' is now hidden and all requests to it will be redirected
:
:
[03:11:57] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [146.190.197.169]
[03:12:09] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [15.161.55.89]
[03:12:15] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [206.189.247.132]
[03:12:23] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [18.170.98.205]
: sessions

+----+----------+-----------------+------------+----------+---------------+------------------+
| id | phishlet |    username     |  password  |  tokens  |   remote ip   |       time       |
+----+----------+-----------------+------------+----------+---------------+------------------+
| 1  | o365     | employee1@s.... | [redacted] | captured | 128.107.78.71 | 2024-04-01 03:10 |
+----+----------+-----------------+------------+----------+---------------+------------------+

: ▌
```

What the Bad Actor sees

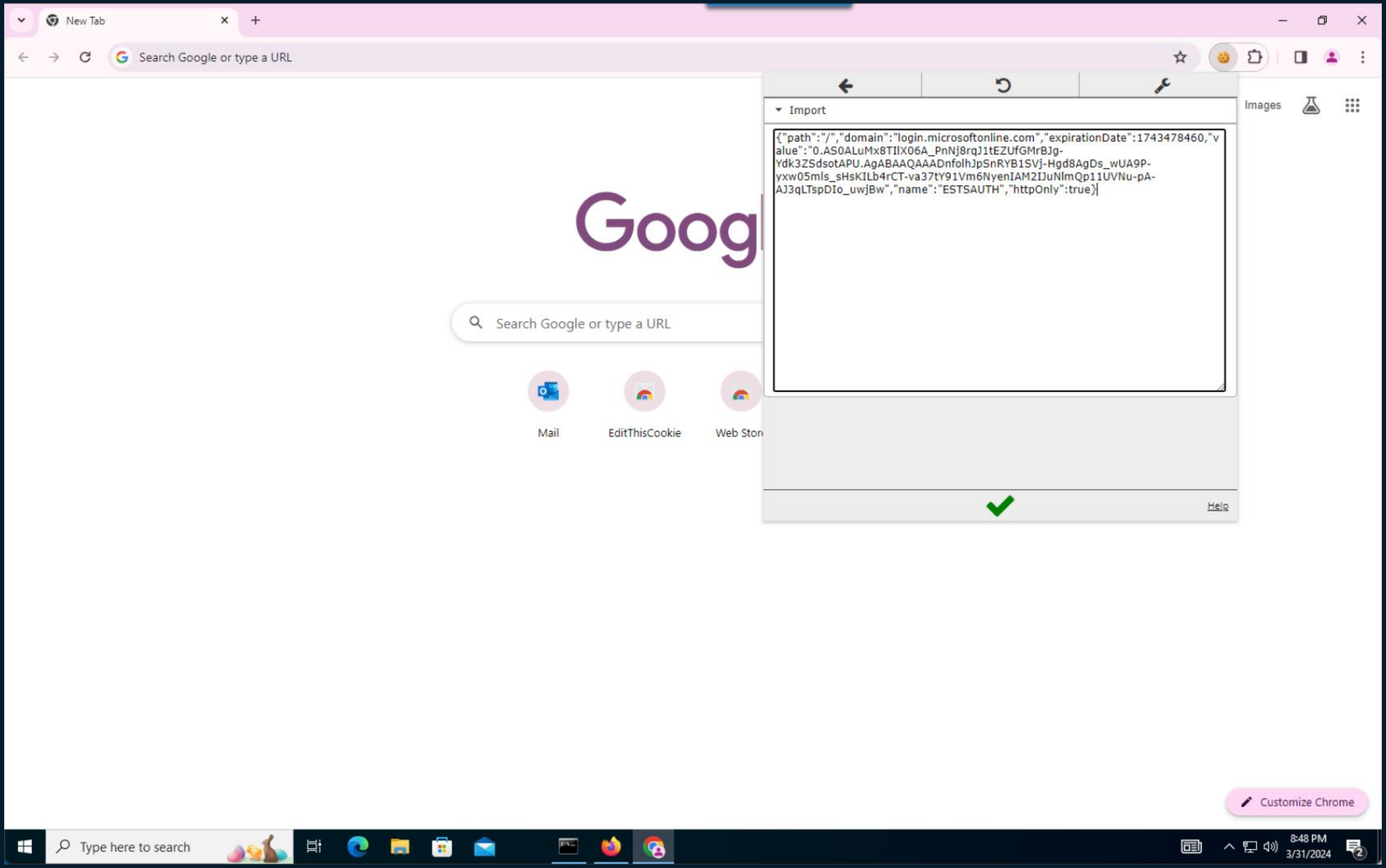


```
[03:09:49] [inf] phishlet 'o365' is now reachable and visible from the outside
:
:
[03:10:03] [imp] [0] [o365] new visitor has arrived: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0 (128.107.78.71)
[03:10:03] [inf] [0] [o365] landing URL: https://login.securitydemo.net/spRqqIiF
[03:10:54] [+++] [0] Username: [employee1@securitydemo.net]
[03:10:54] [+++] [0] Username: [employee1@securitydemo.net]
[03:10:54] [+++] [0] Password: [redacted]
[03:10:58] [+++] [0] all authorization tokens intercepted!
: phishlets hide o365
[03:11:49] [inf] phishlet 'o365' is now hidden and all requests to it will be redirected
:
:
[03:11:57] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [146.190.197.169]
[03:12:09] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [15.161.55.89]
[03:12:15] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [206.189.247.132]
[03:12:23] [war] [o365] request to hidden phishlet: https://www.securitydemo.net/ (Mozilla/5.0 DelfiEEwww/613.0.0 EmbeddedBrowser (iPhone; CPU iPhone OS 17_3_1 like Mac OS X) AppleWebKit (KHTML, like Gecko) Mobile
DeviceUID:  VendorUID:  AppPkgID: ee.delfi.delfi) [18.170.98.205]
: sessions

+----+----------+-----------------+----------+----------+----------------+------------------+
| id | phishlet |    username     | password |  tokens  |   remote ip    |       time       |
+----+----------+-----------------+----------+----------+----------------+------------------+
| 1  | o365     | employee1@s.... | [redacted] | captured | 128.107.78.71 | 2024-04-01 03:10 |
+----+----------+-----------------+----------+----------+----------------+------------------+

: sessions 1

 id           : 1
 phishlet     : o365
 username     : employee1@securitydemo.net
 password     : [redacted]
 tokens       : captured
 landing url  : https://login.securitydemo.net/spRqqIiF
 user-agent   : Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:124.0) Gecko/20100101 Firefox/124.0
 remote ip    : 128.107.78.71
 create time  : 2024-04-01 03:10
 update time  : 2024-04-01 03:10

[ cookies ]
[{"path":"/","domain":"login.microsoftonline.com","expirationDate":1743477211,"value":"CAgABAAIAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-tRhqxiz-AvTv0xkYVxwWi40BKnZi5jNOGMq6j4gIWu-zbsMfG1ysrU-IHo2chjqy6KagCrp2BvKgU62E-Er
Augc6qqho2K40FppZ7VWbCRHxj0pW7wo8Zno6yd67rVGNqYX5PzZyQh4La8ahIb7K8mXLR621ndEmEuK7GiabXuIDNgf_QV08gXZ5MS1NbeiDoR86mIEjF29l0dfA2er_mZaKKiL_DpRREGWxcnT3cmfkN2YA1mbL_ZSrU1de3TVFQK8RP","name":"SignInStateCookie","httpOn
ly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1743477211,"value":"0.AS0ALuMx8TIlX06A_PnNj8rqJ1tEZUfGMrBJg-Ydk3ZSdsotAPU.AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-yxw05mls_sHsKILb4rCT-
va37tY91Vm6NyenIAM2IJuNlmQp11UVNu-pA-AJ3qLTspDIo_uwjBw","name":"ESTSAUTH","httpOnly":true},{"path":"/","domain":"login.microsoftonline.com","expirationDate":1743477211,"value":"0.AS0ALuMx8TIlX06A_PnNj8rqJ1tEZUfGMrB
Jg-Ydk3ZSdsotAPU.AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P9jyXtu1unhZ6-WMQldo7uwW4flc8AnxOZae0dazr0cbcQzSodSk_uSkAueeQhyBL87gmfvTmQ971yCyF088s2MI09xL6jmVNJVWnhb9_XWbPNYki89n78xncTxRHrfPv3DeggjvxHUra-fIkTJb-7m0a4DR
cPlN3haUPGmI3XRVTl8OWWZSH-CenP7ecHmPLGTfu-dOhE0LILBz3U-JV8nPXkJarHbbk2jXRVSgvKVneffrwFm5ZXGNRvkP7jtGCBHko4EERRjnFPZOj-Z6cB4-kpvKwAbDMQXgqlsx4YiTCL1HNXcvc_cgTqJj3NKlnp1TRQckcT-71OvLHoEw1Fo2kepny5xaxS1Tl8zB_1rwaL1rig
XWxZ4ZFmTz8isE7Ol3LcFVKzkpNSQo9XdfGvX7pjpFLDisV_rugEp29Il5LpqSsUMzZ0nHAw9_tN0JyDIxXHbsmZ4EuNBMMVNsnjsStDv3zNwYMUqczs-V_xrUWrFXU8Ix8oQbUI7vN6n7hdflbT494YvyDINcdpQhc2QcI6uksUjNIW8CaV0TDo7B5fJiiee_FKTS7KzHr7qxy3y1ye-W
XzHdF0ELa4QfHzXqU1TDdAFb-EQmqLfqEFqUTXgVwIHqMxTQ_na6WfynZX2MZvNoitQP_E","name":"ESTSAUTHPERSISTENT","httpOnly":true}]

: █
```

Bad Guy sees everything

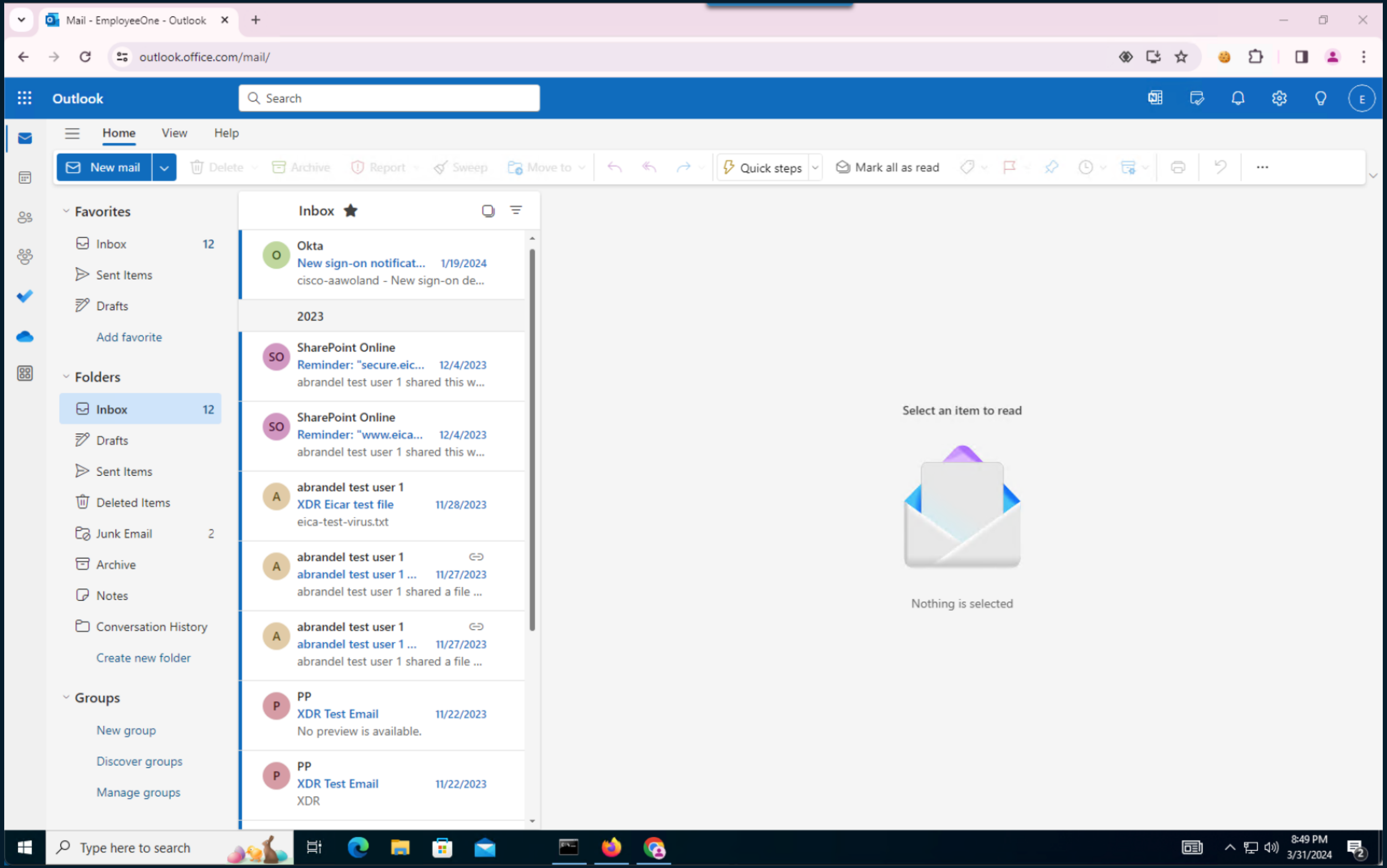
The bad guy is able to capture the username, password (most times) & more importantly the Session Info, including the cookies

Paste the Cookies into a plugin



```
{"path":"/","domain":"login.microsoftonline.com","expirationDate":1743478460,"v
alue":"0.AS0ALuMx8TIlX06A_PnNj8rqJ1tEZUfGMrBJg-
Ydk3ZSdsotAPU.AgABAAQAAADnfolhJpSnRYB1SVj-Hgd8AgDs_wUA9P-
yxw05mls_sHsKILb4rCT-va37tY91Vm6NyenIAM2IJuNlmQp11UVNu-pA-
AJ3qLTspDIo_uwjBw","name":"ESTSAUTH","httpOnly":true}
```

Bam: Access as Employee1



Mail - EmployeeOne - Outlook

outlook.office.com/mail/

Inbox

Okta New sign-on notificat... cisco-aawoland - New sign-on de...	1/19/2024
2023	
SharePoint Online Reminder: "secure.eic... abrandel test user 1 shared this w...	12/4/2023
SharePoint Online Reminder: "www.eica... abrandel test user 1 shared this w...	12/4/2023
abrandel test user 1 XDR Eicar test file eica-test-virus.txt	11/28/2023
abrandel test user 1 abrandel test user 1 ... abrandel test user 1 shared a file ...	11/27/2023
abrandel test user 1 abrandel test user 1 ... abrandel test user 1 shared a file ...	11/27/2023
PP XDR Test Email No preview is available.	11/22/2023
PP XDR Test Email XDR	11/22/2023

Select an item to read

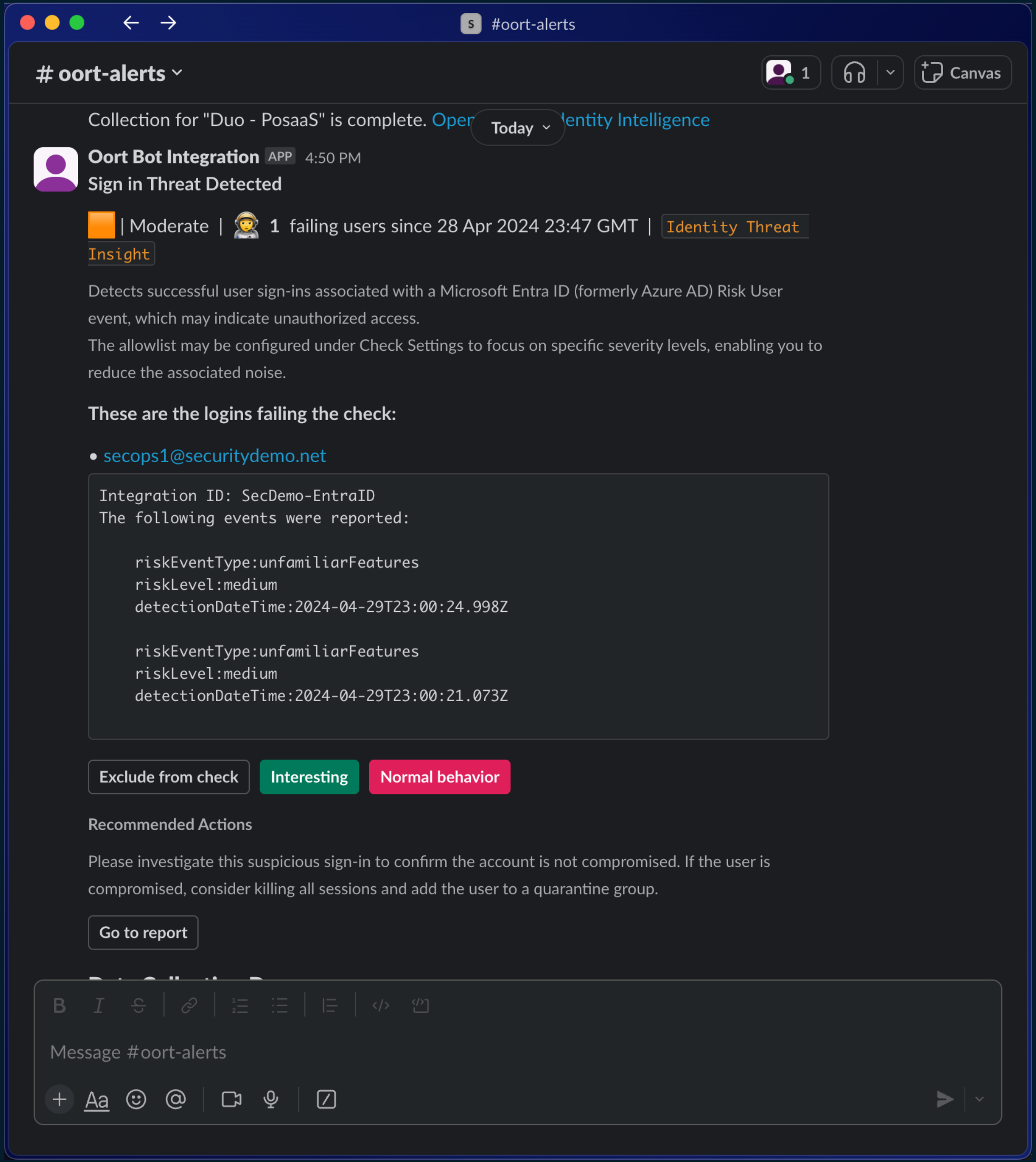
Nothing is selected

Technical Nuggets

- With event-streaming, this gets detected much faster than Graph API sync
  - These signals from Entra fall into what are called “real-time checks”
  - Really near-real-time ☺
- Without event streaming it can take over 24 hours to detect this, if at all
- Entra ID will label these as “Medium" criticality events, even though it was a successful attack
  - Still testing w/ Okta and other IDPs to see how they categorize it
  - Okta shares the session info in their logs & makes it easier to detect

Bam! Detected & Alerted

- All notification channels for the check will have gotten a message:
    - ChatOps / IM channels
    - Webhooks
    - Emails, etc.
- SOAR, XDR & other automation tools can begin work automatically
    - Or manual investigations can start in response to the notification



Collection for "Duo - PosaaS" is complete. Oper dentity Intelligence

Oort Bot Integration 4:50 PM

Sign in Threat Detected

🟧 | Moderate | 1 failing users since 28 Apr 2024 23:47 GMT | `Identity Threat Insight`

Detects successful user sign-ins associated with a Microsoft Entra ID (formerly Azure AD) Risk User event, which may indicate unauthorized access.
The allowlist may be configured under Check Settings to focus on specific severity levels, enabling you to reduce the associated noise.

These are the logins failing the check:

- secops1@securitydemo.net

```
Integration ID: SecDemo-EntraID
The following events were reported:

    riskEventType:unfamiliarFeatures
    riskLevel:medium
    detectionDateTime:2024-04-29T23:00:24.998Z

    riskEventType:unfamiliarFeatures
    riskLevel:medium
    detectionDateTime:2024-04-29T23:00:21.073Z
```

Recommended Actions

Please investigate this suspicious sign-in to confirm the account is not compromised. If the user is compromised, consider killing all sessions and add the user to a quarantine group.

Remediation from Cisco Identity Intelligence

Taking Action(s)

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

- Organizations have invested heavily in their response flows with ticketing systems like Service Now, 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

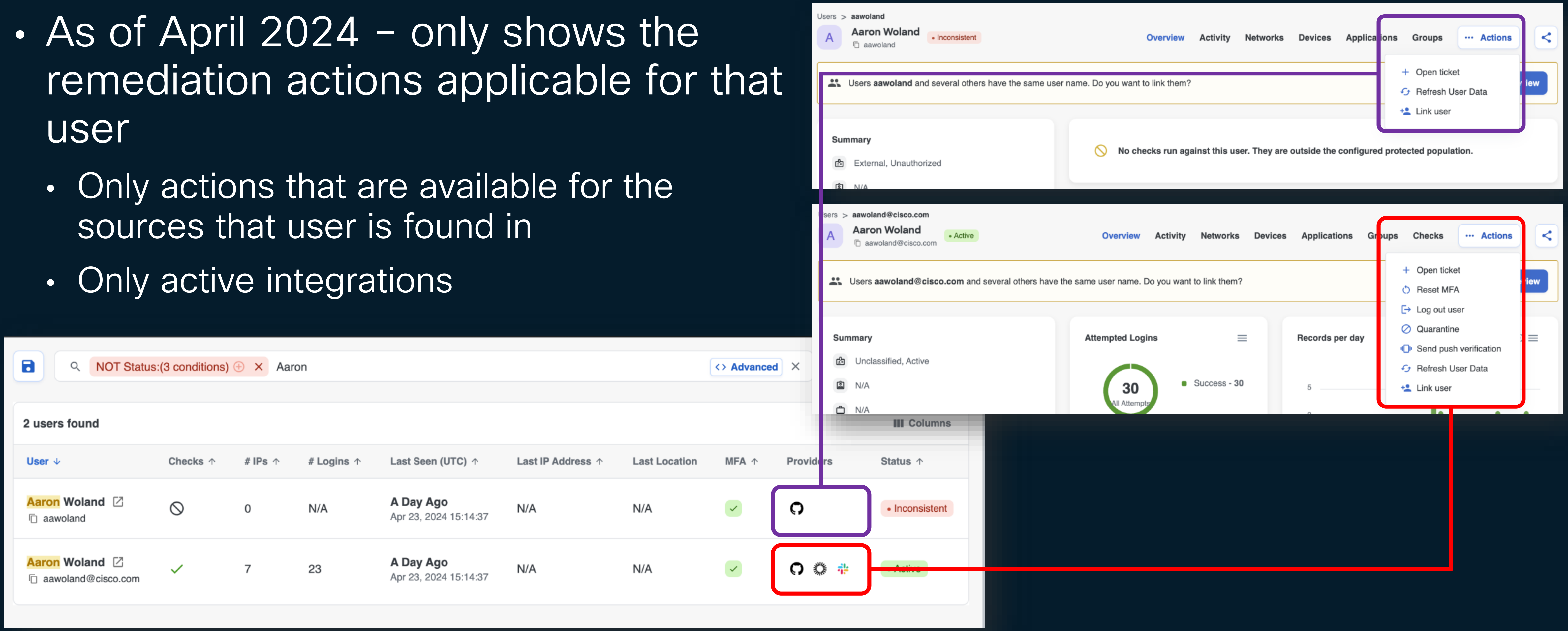
- Not all sources support the same remediation.
- Reset MFA is applicable to Okta & Duo only (for example)

Remediation Nuggets:

- CII only allows one remediation action at a time.
- The provider must be configured to allow the actions (think "*write*" access)
- Some remediations require setup on the IDP side (see docs).

Context Specific Remediation Menu

- As of April 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



Users **aawoland** and several others have the same user name. Do you want to link them?

External, Unauthorized

N/A

No checks run against this user. They are outside the configured protected population.

Users **aawoland@cisco.com** and several others have the same user name. Do you want to link them?

Unclassified, Active

N/A

N/A

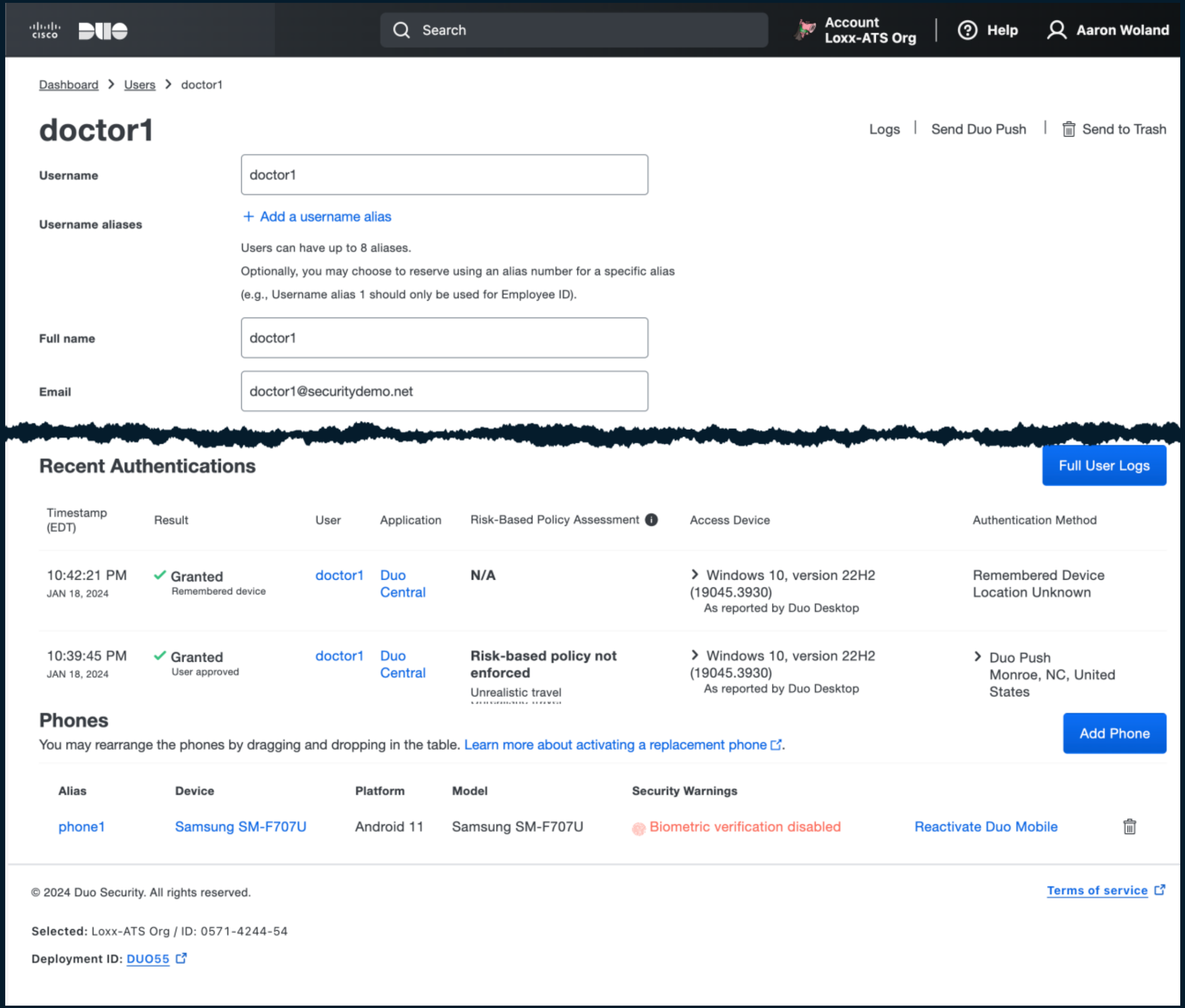
2 users found

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

Reset MFA

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



Dashboard > Users > doctor1

doctor1

Logs | Send Duo Push | Send to Trash

Username	doctor1
Username aliases	+ Add a username alias Users can have up to 8 aliases. Optionally, you may choose to reserve using an alias number for a specific alias (e.g., Username alias 1 should only be used for Employee ID).
Full name	doctor1
Email	doctor1@securitydemo.net

Recent Authentications

Full User Logs

Timestamp (EDT)	Result	User	Application	Risk-Based Policy Assessment	Access Device	Authentication Method
10:42:21 PM JAN 18, 2024	✓ Granted Remembered device	doctor1	Duo Central	N/A	> Windows 10, version 22H2 (19045.3930) As reported by Duo Desktop	Remembered Device Location Unknown
10:39:45 PM JAN 18, 2024	✓ Granted User approved	doctor1	Duo Central	Risk-based policy not enforced Unrealistic travel	> Windows 10, version 22H2 (19045.3930) As reported by Duo Desktop	> Duo Push Monroe, NC, United States

Phones

You may rearrange the phones by dragging and dropping in the table. Learn more about activating a replacement phone.

Add Phone

Alias	Device	Platform	Model	Security Warnings		
phone1	Samsung SM-F707U	Android 11	Samsung SM-F707U	Biometric verification disabled	Reactivate Duo Mobile	🗑

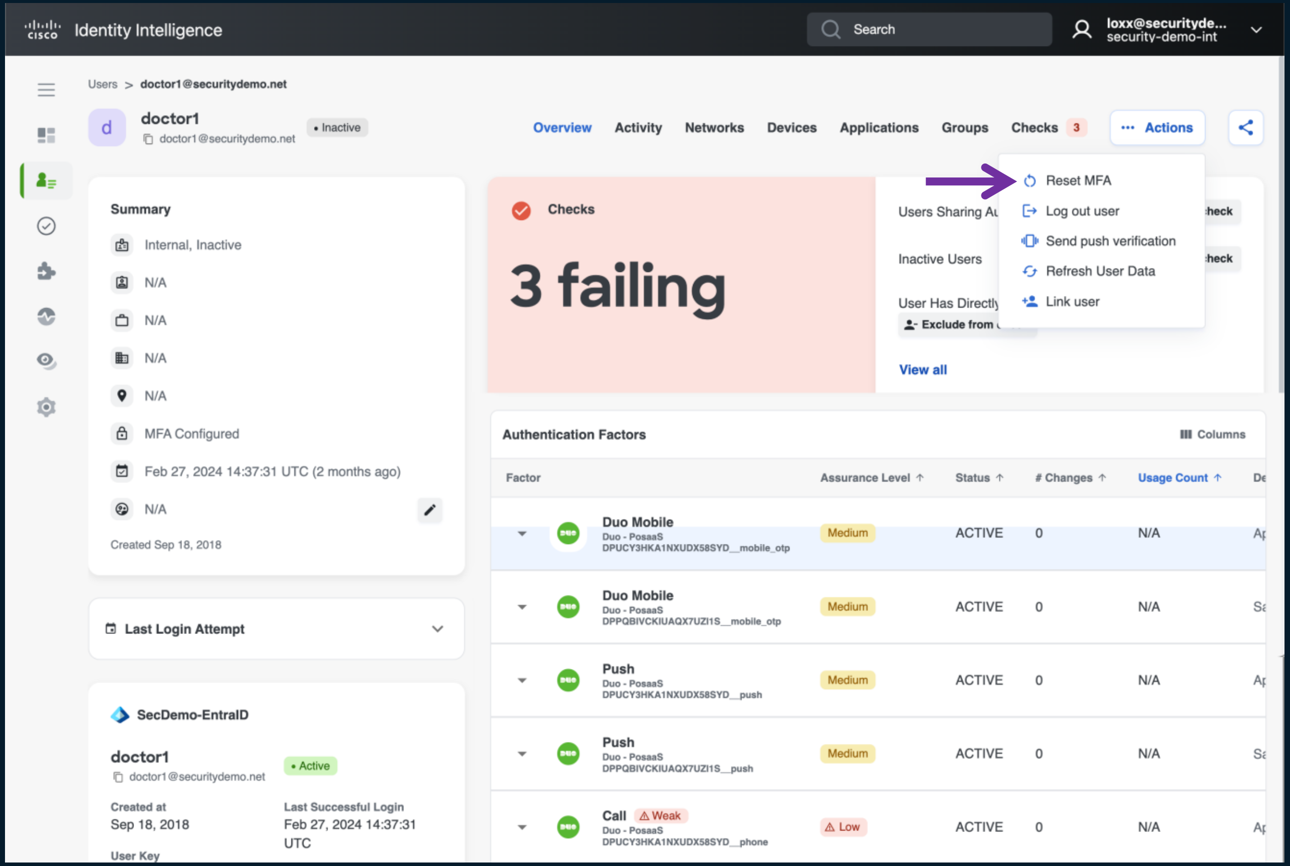
© 2024 Duo Security. All rights reserved.

Terms of service

Selected: Loxx-ATS Org / ID: 0571-4244-54

Deployment ID: DUO55

Duo’s Reset MFA



Summary

Internal, Inactive

N/A

N/A

N/A

N/A

MFA Configured

Feb 27, 2024 14:37:31 UTC (2 months ago)

N/A

Created Sep 18, 2018

Last Login Attempt

SecDemo-EntraID

doctor1 • Active

doctor1@securitydemo.net

Created at: Sep 18, 2018

Last Successful Login: Feb 27, 2024 14:37:31 UTC

User Key

Checks

3 failing

Users Sharing Au

Inactive Users

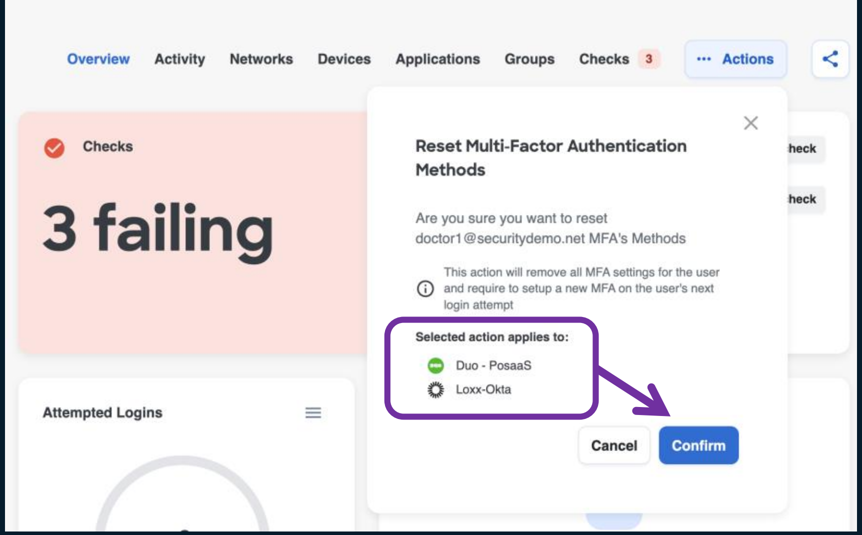
User Has Directly

Exclude from

View all

Authentication Factors

Factor	Assurance Level ↑	Status ↑	# Changes ↑	Usage Count ↑	De
Duo Mobile Duo - PosaaS DPUCY3HKA1NXUDX58SYD__mobile_otp	Medium	ACTIVE	0	N/A	Ap
Duo Mobile Duo - PosaaS DPPQBIVCKIUAQX7UZI1S__mobile_otp	Medium	ACTIVE	0	N/A	Sa
Push Duo - PosaaS DPUCY3HKA1NXUDX58SYD__push	Medium	ACTIVE	0	N/A	Ap
Push Duo - PosaaS DPPQBIVCKIUAQX7UZI1S__push	Medium	ACTIVE	0	N/A	Sa
Call ⚠ Weak Duo - PosaaS DPUCY3HKA1NXUDX58SYD__phone	⚠ Low	ACTIVE	0	N/A	Ap



Reset Multi-Factor Authentication Methods

Are you sure you want to reset doctor1@securitydemo.net MFA's Methods

This action will remove all MFA settings for the user and require to setup a new MFA on the user's next login attempt

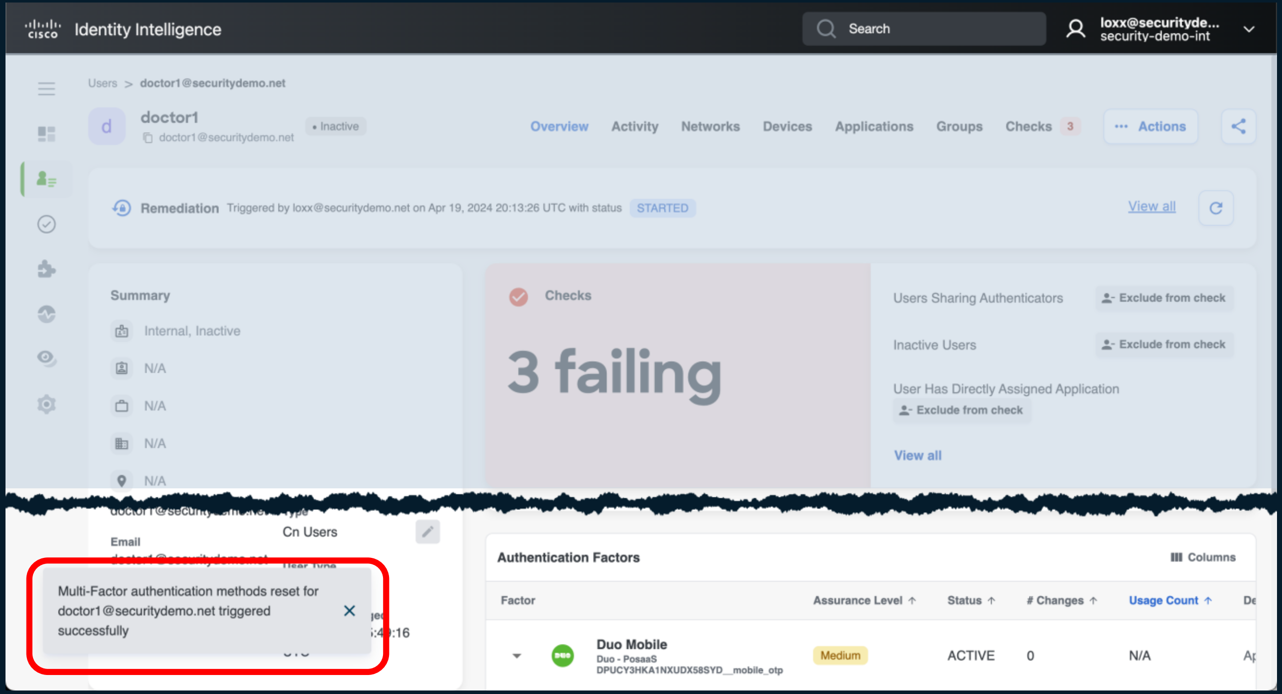
Selected action applies to:

Duo - PosaaS

Loxx-Okta

Cancel | Confirm

Remediation – Duo’s Reset MFA



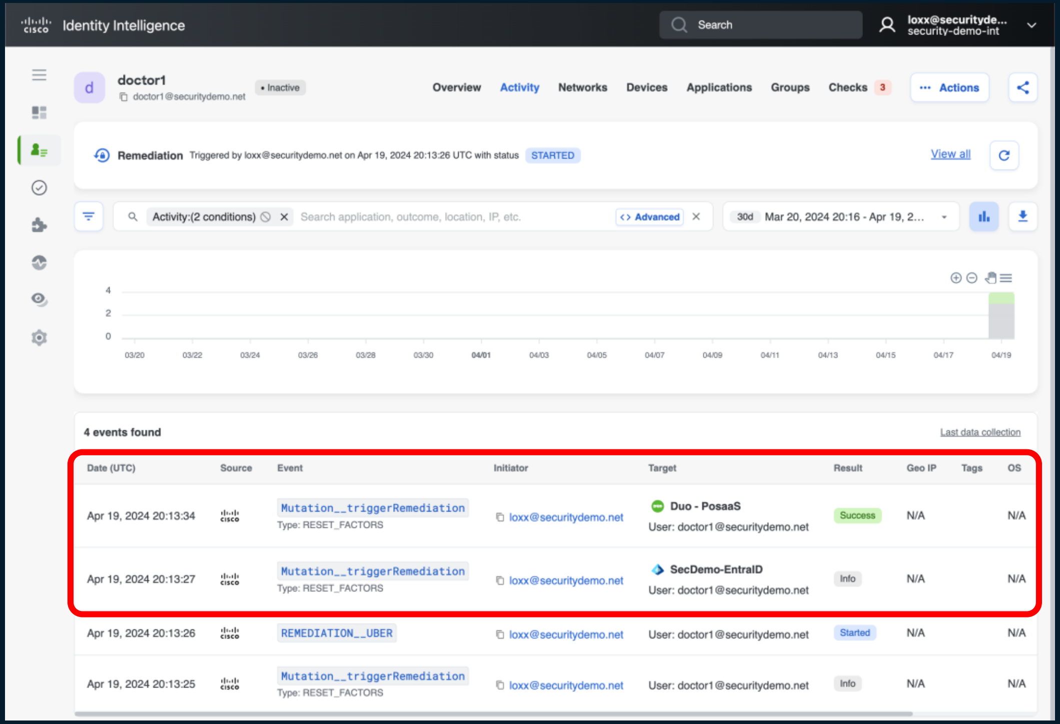
Remediation Triggered by loxx@securitydemo.net on Apr 19, 2024 20:13:26 UTC with status STARTED

3 failing

Multi-Factor authentication methods reset for doctor1@securitydemo.net triggered successfully

Authentication Factors

Factor	Assurance Level ↑	Status ↑	# Changes ↑	Usage Count ↑
Duo Mobile Duo - PosaaS DPUCY3HKA1NXUDX58SYD__mobile_otp	Medium	ACTIVE	0	N/A



Remediation Triggered by loxx@securitydemo.net on Apr 19, 2024 20:13:26 UTC with status STARTED

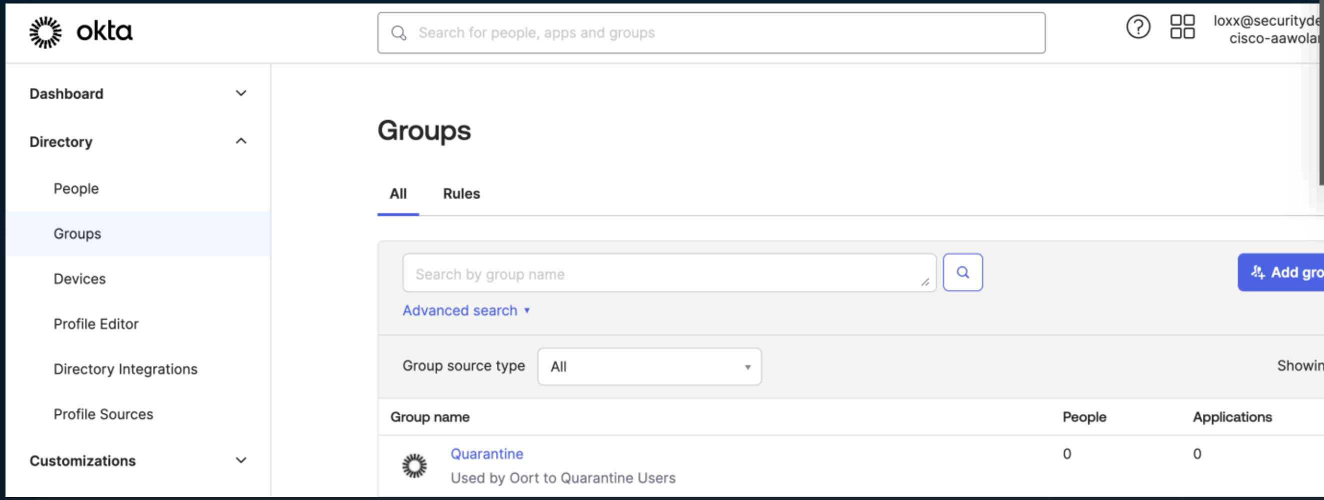
4 events found

Date (UTC)	Source	Event	Initiator	Target	Result	Geo IP	Tags	OS
Apr 19, 2024 20:13:34	cisco	Mutation__triggerRemediation Type: RESET_FACTORS	loxx@securitydemo.net	Duo - PosaaS User: doctor1@securitydemo.net	Success	N/A		N/A
Apr 19, 2024 20:13:27	cisco	Mutation__triggerRemediation Type: RESET_FACTORS	loxx@securitydemo.net	SecDemo-EntraID User: doctor1@securitydemo.net	Info	N/A		N/A
Apr 19, 2024 20:13:26	cisco	REMEDIATION__UBER	loxx@securitydemo.net	User: doctor1@securitydemo.net	Started	N/A		N/A
Apr 19, 2024 20:13:25	cisco	Mutation__triggerRemediation Type: RESET_FACTORS	loxx@securitydemo.net	User: doctor1@securitydemo.net	Info	N/A		N/A

Quarantine User

Quarantine User with Okta

- Must have an Okta group named "Quarantine"
  - Group must be associated with polices and rules that take precedence



okta

Search for people, apps and groups

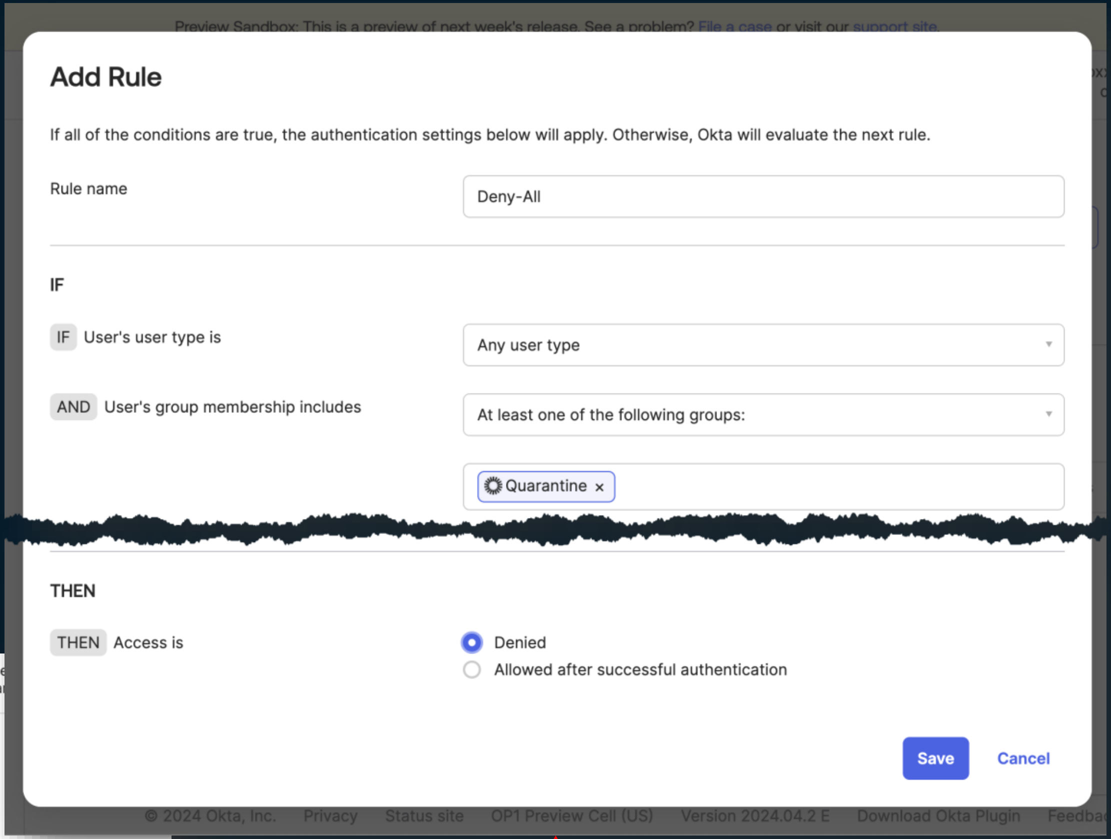
loxx@securityde
cisco-aawolai

Groups

Group source type: All

Showing 25

Group name	People	Applications
Quarantine Used by Oort to Quarantine Users	0	0



Preview Sandbox: This is a preview of next week's release. See a problem? File a case or visit our support site.

Add Rule

If all of the conditions are true, the authentication settings below will apply. Otherwise, Okta will evaluate the next rule.

Rule name: Deny-All

IF

IF User's user type is: Any user type

AND User's group membership includes: At least one of the following groups:

Quarantine ×

THEN

THEN Access is

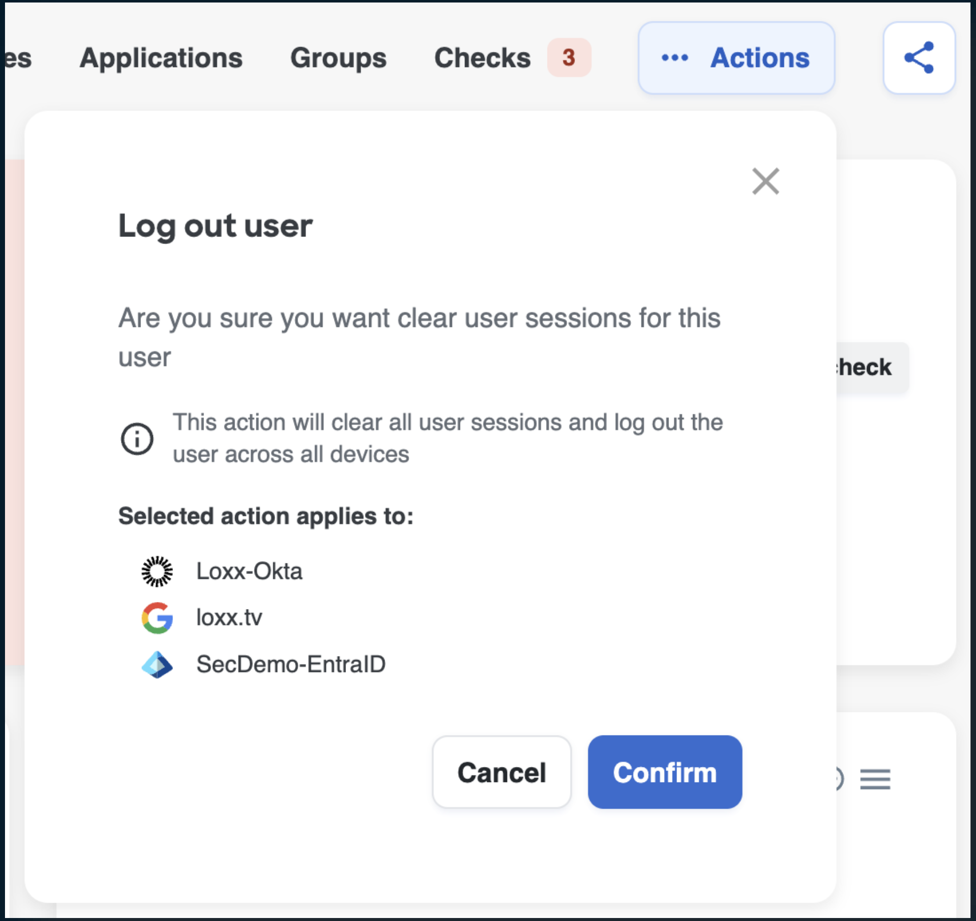
● Denied
○ Allowed after successful authentication

© 2024 Okta, Inc. Privacy Status site OP1 Preview Cell (US) Version 2024.04.2 E Download Okta Plugin Feedba okta Google Workspace Microsoft Azure

Log User Out of Active Sessions

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



Log out user

Are you sure you want clear user sessions for this user

This action will clear all user sessions and log out the user across all devices

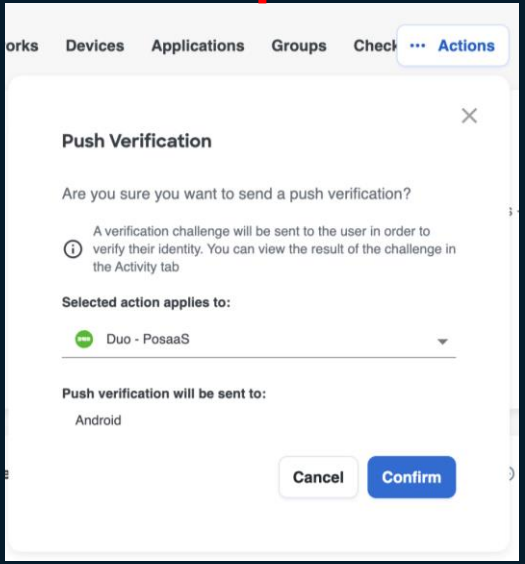
Selected action applies to:

Loxx-Okta
loxx.tv
SecDemo-EntraID

Send Push Notification

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



Push Verification

Are you sure you want to send a push verification?

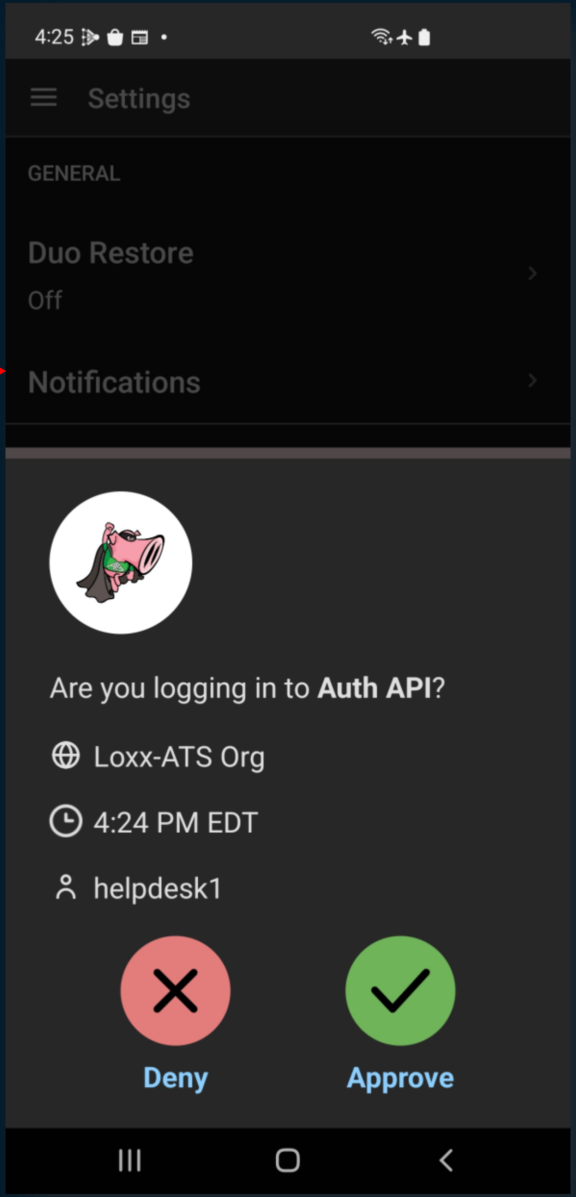
ⓘ A verification challenge will be sent to the user in order to verify their identity. You can view the result of the challenge in the Activity tab

Selected action applies to:

Duo - PosaaS

Push verification will be sent to:

Android



Are you logging in to **Auth API**?

Loxx-ATS Org

4:24 PM EDT

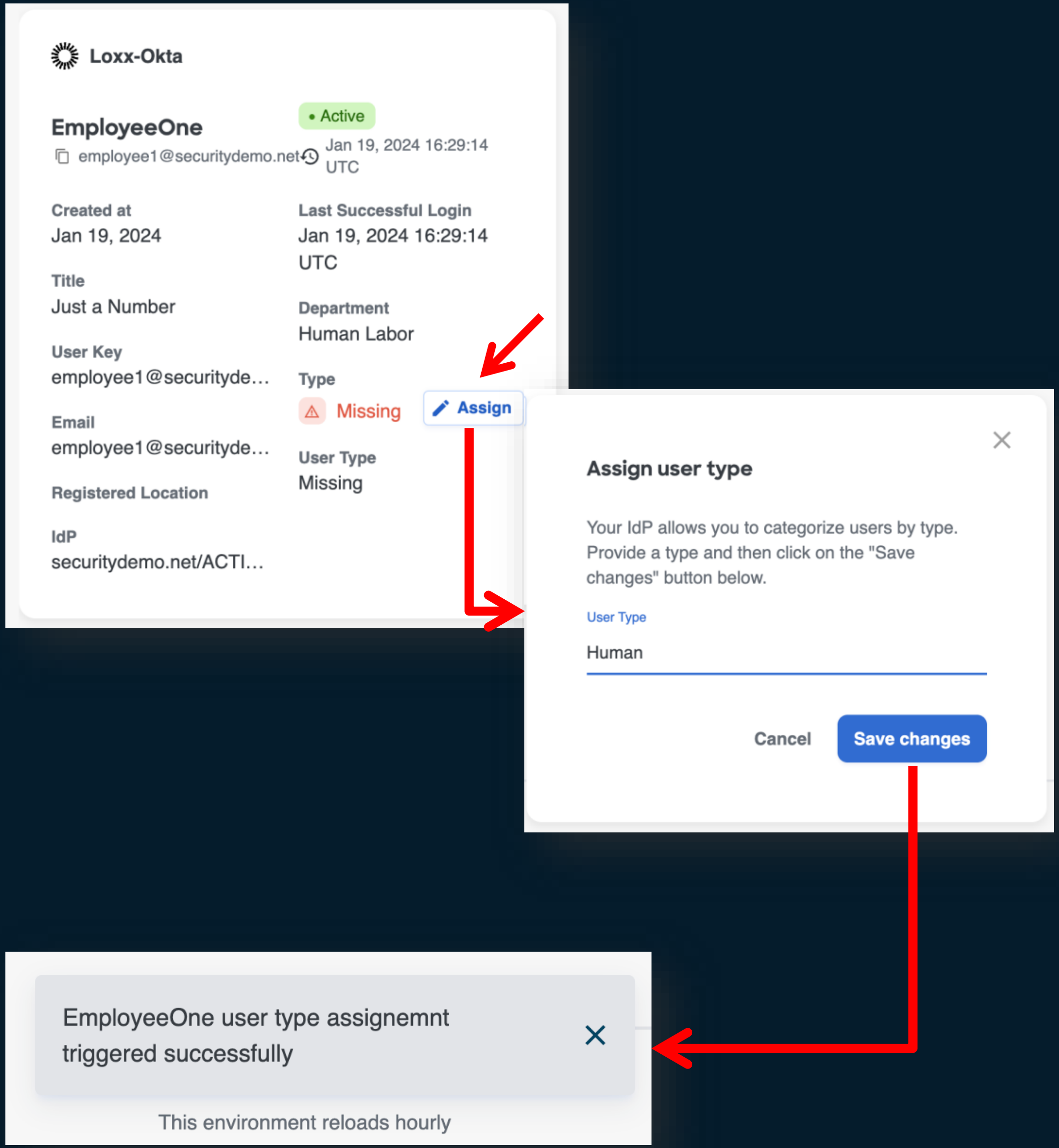
helpdesk1

okta Microsoft Azure

Update User Type

Update User Type

- Okta & Azure have a concept of a “User-Type”
  - Employee
  - Contractor
  - Intern
  - etc.
- If the type isn’t sync’d into the IDP, you can assign from CII



Loxx-Okta

EmployeeOne
employee1@securitydemo.net

• Active
Jan 19, 2024 16:29:14 UTC

Created at
Jan 19, 2024

Last Successful Login
Jan 19, 2024 16:29:14 UTC

Title
Just a Number

Department
Human Labor

User Key
employee1@securityde…

Type
Missing

Email
employee1@securityde…

User Type
Missing

Registered Location

IdP
securitydemo.net/ACTI…

Assign user type

Your IdP allows you to categorize users by type. Provide a type and then click on the "Save changes" button below.

User Type
Human

EmployeeOne user type assignemnt triggered successfully

This environment reloads hourly

Other Technical Nuggets

Types of Data

Behavioral Data

- Devices, IPs, Location Prevalence, etc.
- Used for identifying abnormal behavior

Event Data

- Authentication logs
- Alerts
- Audit logs
- Provisioning Logs
- Risky user events

Directory Data

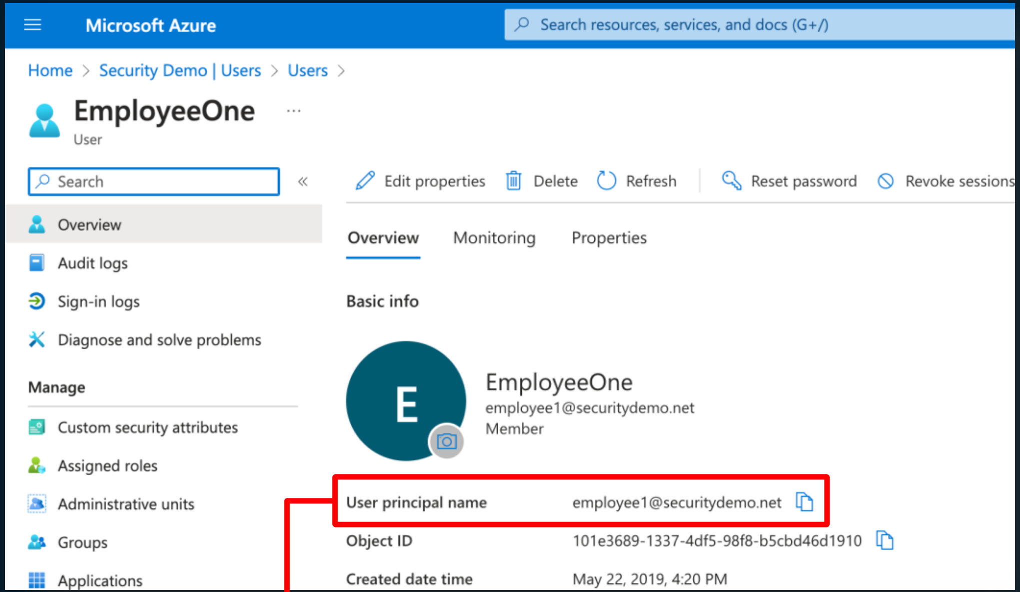
- The list of users, their attributes & properties
- Groups, & group memberships
- Hierarchy’s

CII pulls that bulk data from the API(s)

- The events & CRUD notifications are used to keep the data up-2-date
- There is a monthly “rebase” to ensure the full data is correctly in sync.

Account Merges

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



Microsoft Azure

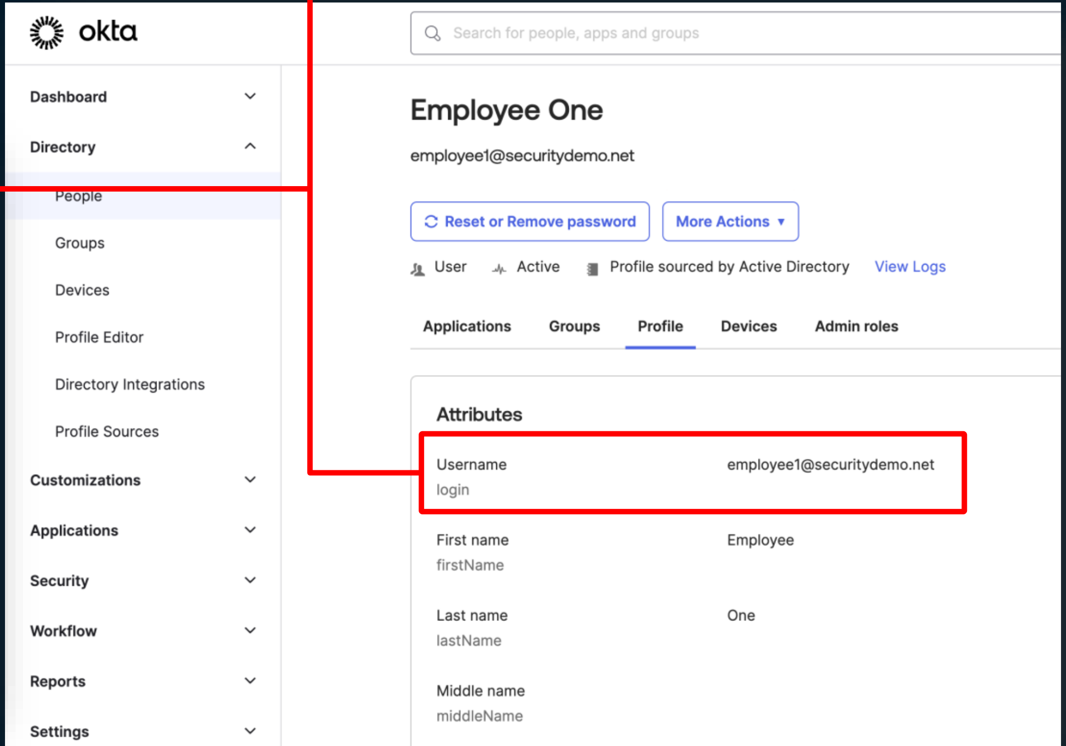
Home > Security Demo | Users > Users >

EmployeeOne
User

Basic info

EmployeeOne
employee1@securitydemo.net
Member

User principal name	employee1@securitydemo.net
Object ID	101e3689-1337-4df5-98f8-b5cbd46d1910
Created date time	May 22, 2019, 4:20 PM



okta

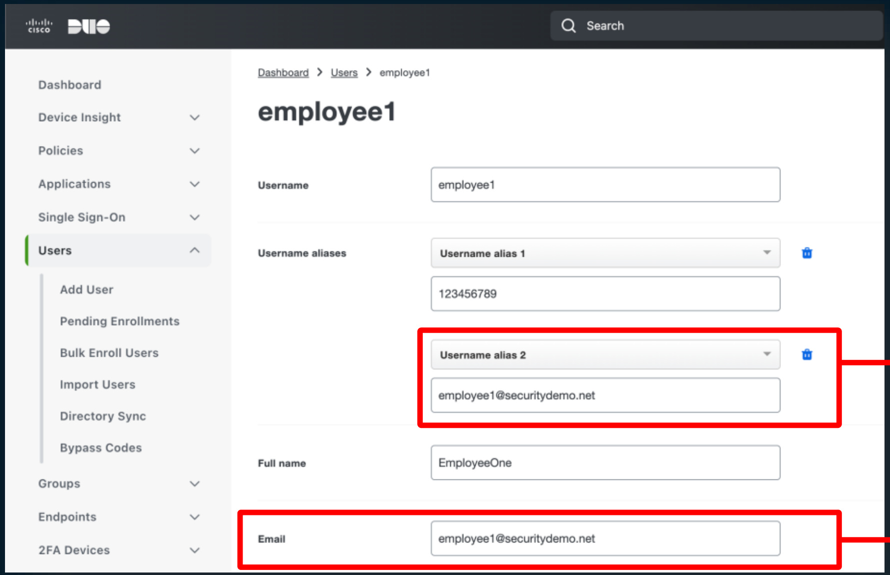
Employee One

employee1@securitydemo.net

User · Active · Profile sourced by Active Directory · View Logs

Attributes

Username login	employee1@securitydemo.net
First name firstName	Employee
Last name lastName	One
Middle name middleName	



DUO

Dashboard > Users > employee1

employee1

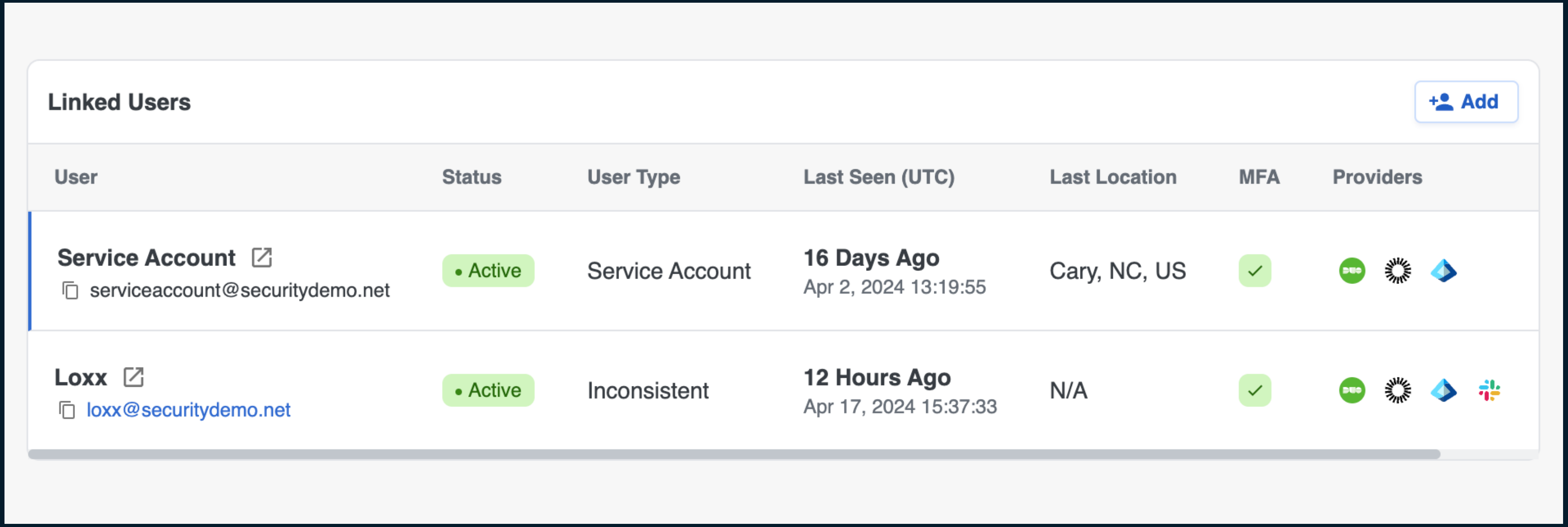
Username	employee1
Username aliases	Username alias 1 123456789 Username alias 2 employee1@securitydemo.net
Full name	EmployeeOne
Email	employee1@securitydemo.net

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

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

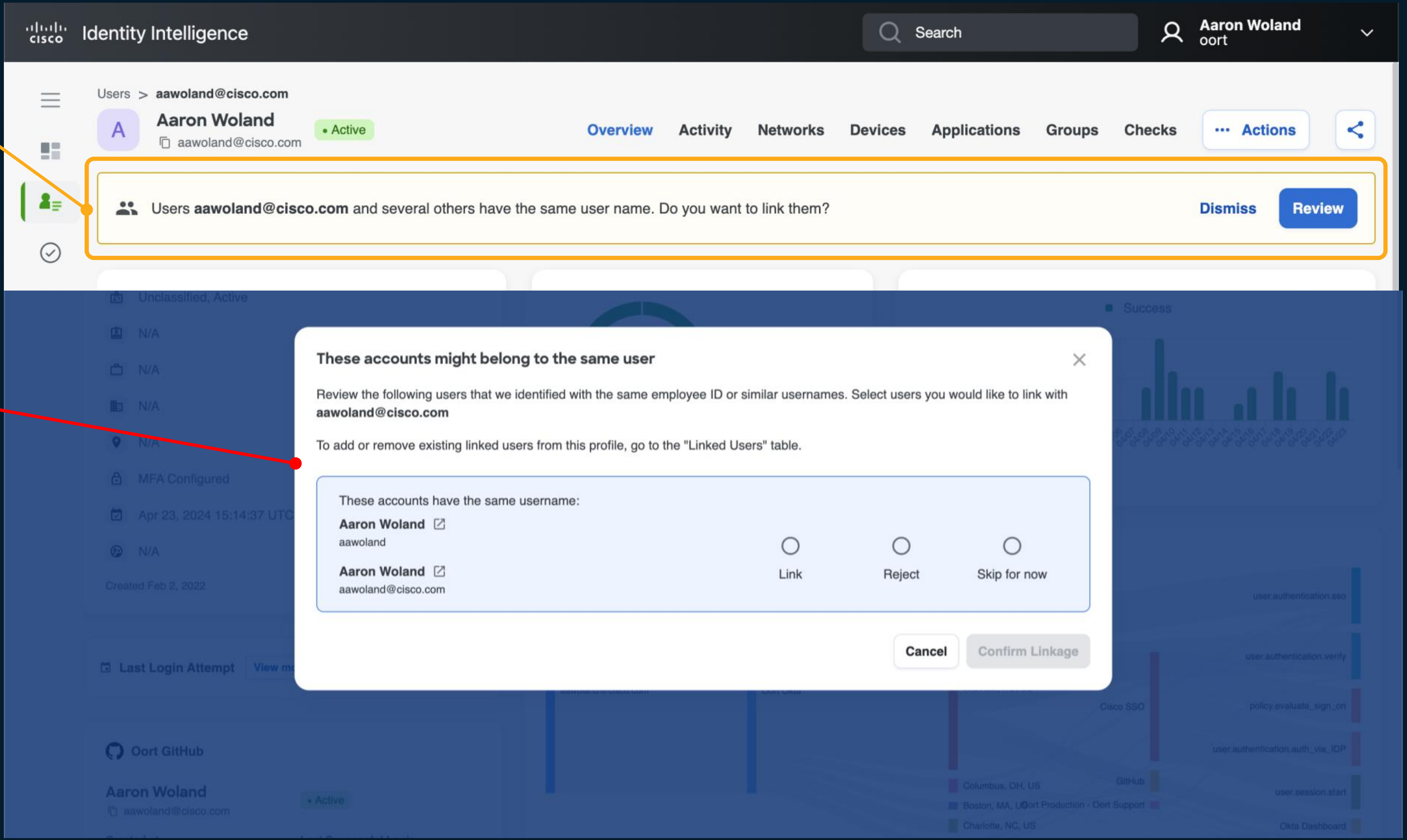
CII will merge accounts automatically.

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



Users **aawoland@cisco.com** and several others have the same user name. Do you want to link them?

These accounts might belong to the same user

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**

To add or remove existing linked users from this profile, go to the "Linked Users" table.

These accounts have the same username:

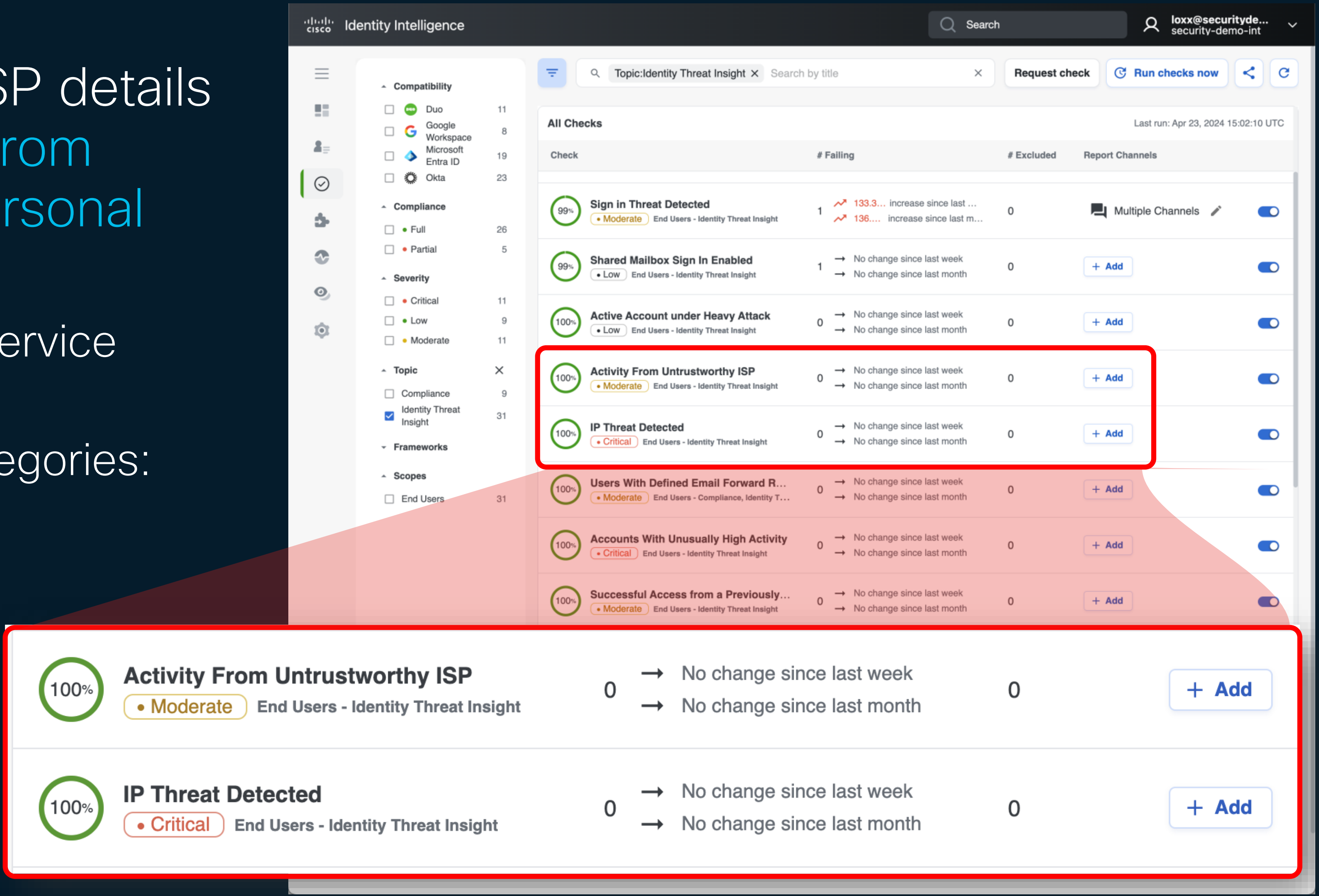
Aaron Woland
aawoland

Aaron Woland
aawoland@cisco.com

○ Link ○ Reject ○ Skip for now

Threat Intel Nuggets

- How Oort 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
    - MaliciousIp
    - PasswordSpray



All Checks

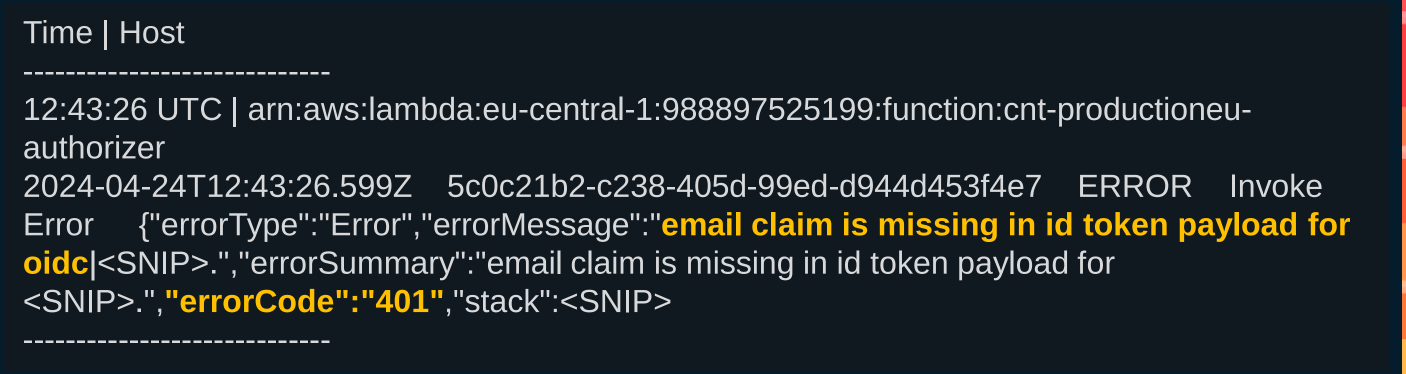
Last run: Apr 23, 2024 15:02:10 UTC

Check	# Failing		# Excluded	Report Channels
99% Sign in Threat Detected • Moderate End Users - Identity Threat Insight	1	133.3... increase since last ... 136.... increase since last m...	0	Multiple Channels
99% Shared Mailbox Sign In Enabled • Low End Users - Identity Threat Insight	1	→ No change since last week → No change since last month	0	+ Add
100% Active Account under Heavy Attack • Low End Users - Identity Threat Insight	0	→ No change since last week → No change since last month	0	+ Add
100% Activity From Untrustworthy ISP • Moderate End Users - Identity Threat Insight	0	→ No change since last week → No change since last month	0	+ Add
100% IP Threat Detected • Critical End Users - Identity Threat Insight	0	→ No change since last week → No change since last month	0	+ Add
100% Users With Defined Email Forward R... • Moderate End Users - Compliance, Identity T...	0	→ No change since last week → No change since last month	0	+ Add
100% Accounts With Unusually High Activity • Critical End Users - Identity Threat Insight	0	→ No change since last week → No change since last month	0	+ Add
100% Successful Access from a Previously... • Moderate End Users - Identity Threat Insight	0	→ No change since last week → No change since last month	0	+ Add

100% Activity From Untrustworthy ISP • Moderate End Users - Identity Threat Insight	0	→ No change since last week → No change since last month	0	+ Add
100% IP Threat Detected • Critical End Users - Identity Threat Insight	0	→ No change since last week → No change since last month	0	+ Add

Miscellaneous Nuggets

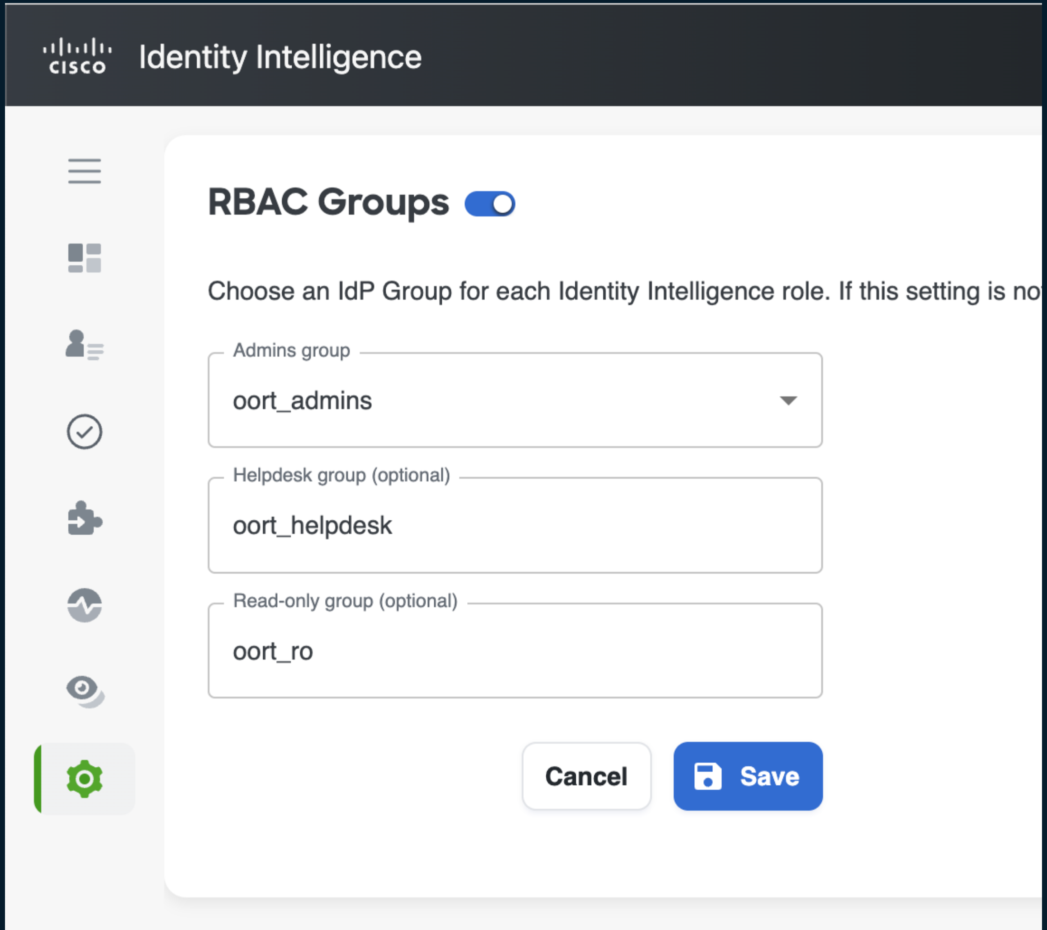
- Email addresses are used as the primary ID of all admins.
  - The OIDC / SAML field is required for the admin logins
  - UPN is not enough
- Security Cloud Sign-on is requiring emails, too.
  - See this error when orgs have privileged accounts that are special (w/o email)
  - Note: It does not have to be a working email



```
Time | Host
----------------------------
12:43:26 UTC | arn:aws:lambda:eu-central-1:988897525199:function:cnt-productioneu-
authorizer
2024-04-24T12:43:26.599Z    5c0c21b2-c238-405d-99ed-d944d453f4e7    ERROR    Invoke
Error    {"errorType":"Error","errorMessage":"email claim is missing in id token payload for
oidc|<SNIP>.","errorSummary":"email claim is missing in id token payload for
<SNIP>.","errorCode":"401","stack":<SNIP>
----------------------------
```

Role Based Access Control

- Three built in Roles:
  - Admins (Full Administrator)
  - Helpdesk
  - Read-only
- CII does not maintain an administrator list
  - Default: All who AuthC/AuthZ successfully via your integrated IDP will be Admins
  - Or, assign IDP groups to the three roles.



RBAC Groups

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

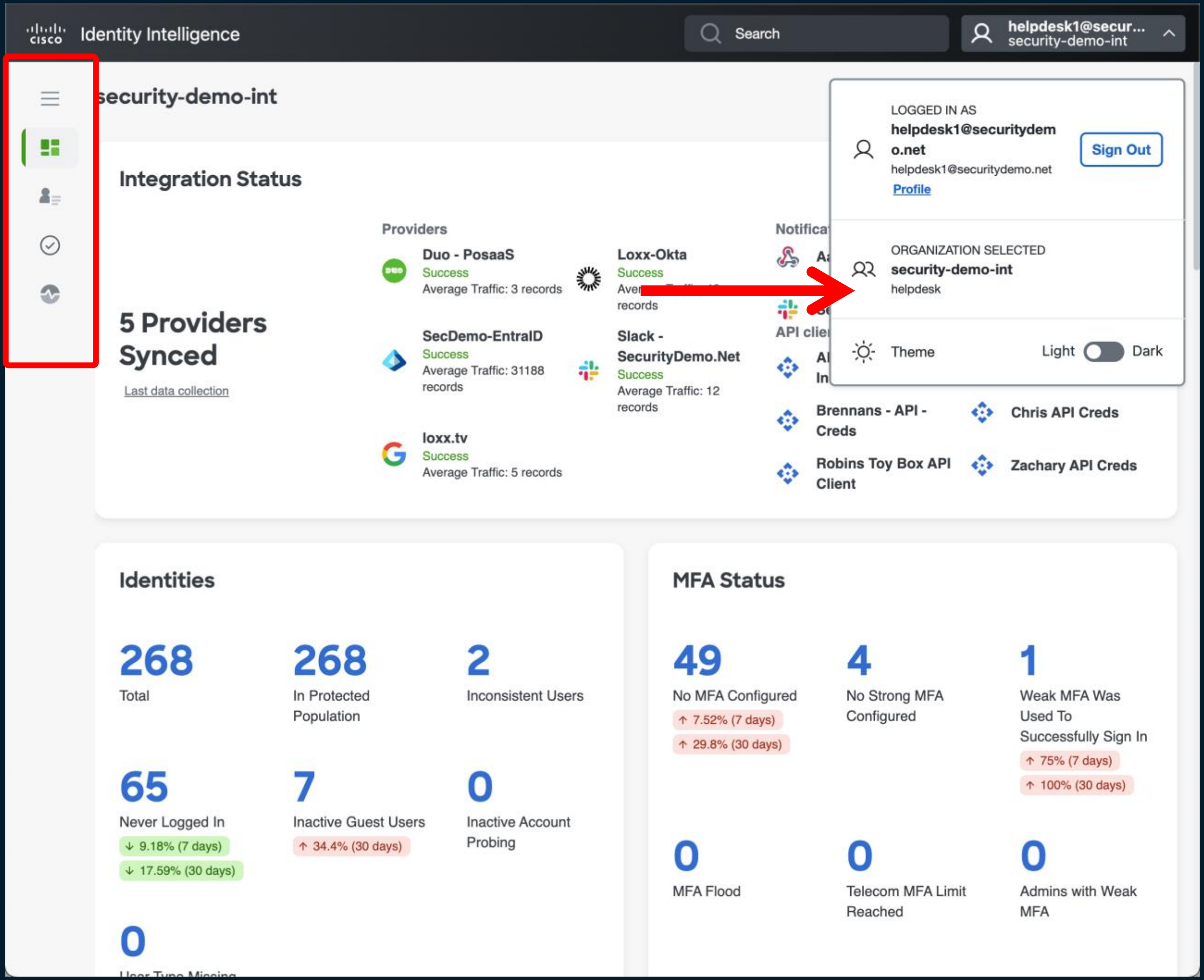
Admins group: oort_admins

Helpdesk group (optional): oort_helpdesk

Read-only group (optional): oort_ro

Role Based Access Control

- Helpdesk
  - No access to Integrations
  - No access to Tenant Settings
  - Tennant Access is also not available
- Is able to take remediation actions
  - Opening tickets
  - Resetting a users MFA
  - Logging a user out of active sessions in one or more IDPs
  - Refreshing user events for troubleshooting



security-demo-int

Integration Status

5 Providers Synced

Last data collection

Providers

Duo - PosaaS
Success
Average Traffic: 3 records

Loxx-Okta
Success
Aver
records

SecDemo-EntraID
Success
Average Traffic: 31188 records

Slack - SecurityDemo.Net
Success
Average Traffic: 12 records

loxx.tv
Success
Average Traffic: 5 records

Notifica

API clie

Brennans - API - Creds

Chris API Creds

Robins Toy Box API Client

Zachary API Creds

LOGGED IN AS
helpdesk1@securitydemo.net
helpdesk1@securitydemo.net
Profile

ORGANIZATION SELECTED
security-demo-int
helpdesk

Theme Light Dark

Identities

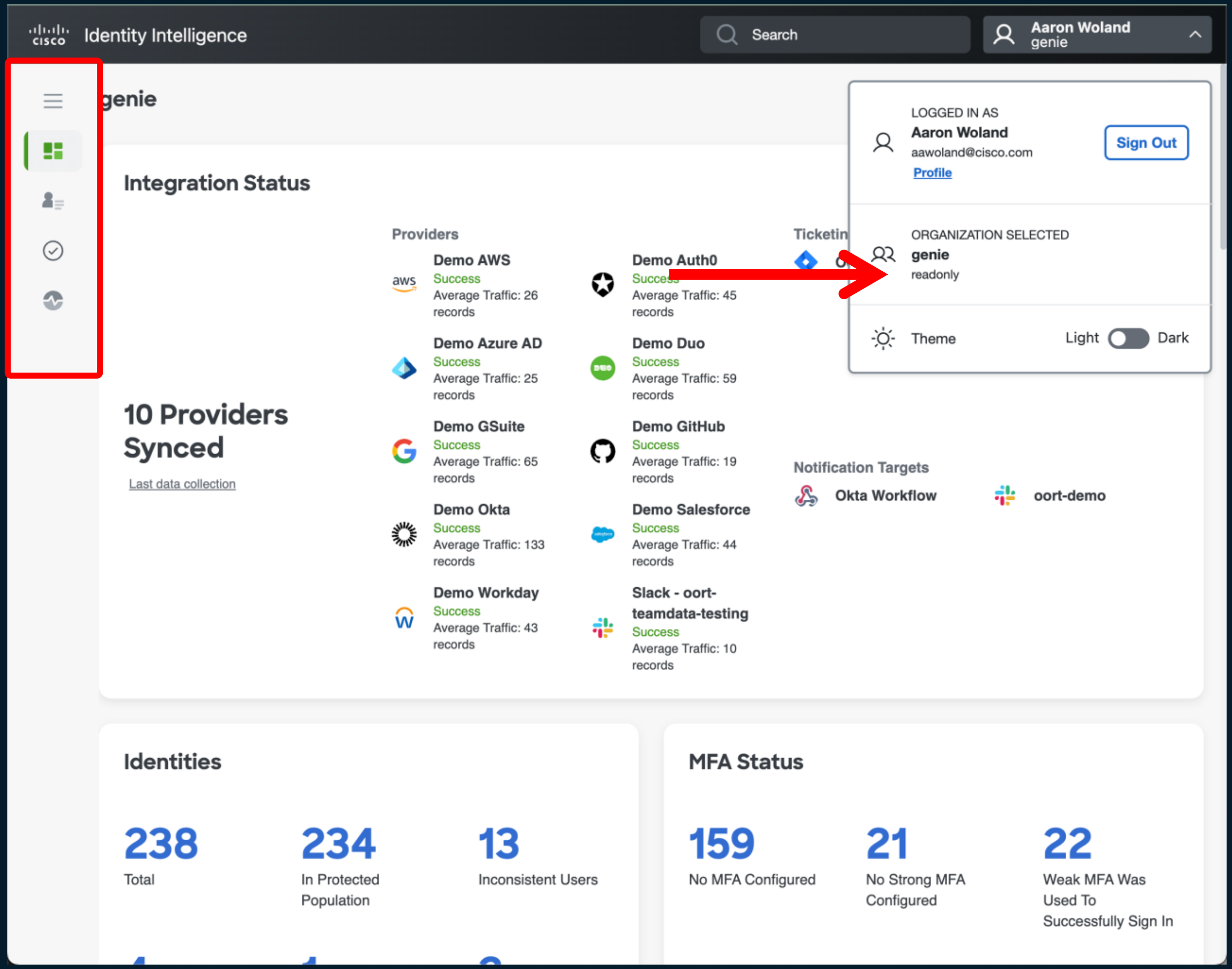
268 Total	268 In Protected Population	2 Inconsistent Users
65 Never Logged In ↓ 9.18% (7 days) ↓ 17.59% (30 days)	7 Inactive Guest Users ↑ 34.4% (30 days)	0 Inactive Account Probing
0 User Type Missing		

MFA Status

49 No MFA Configured ↑ 7.52% (7 days) ↑ 29.8% (30 days)	4 No Strong MFA Configured	1 Weak MFA Was Used To Successfully Sign In ↑ 75% (7 days) ↑ 100% (30 days)
0 MFA Flood	0 Telecom MFA Limit Reached	0 Admins with Weak MFA

Role Based Access Control

- Read-only
  - No access to Integrations
  - No access to Tenant Settings
  - Tennant Access is also not available



Identity Intelligence

Search

Aaron Woland
genie

genie

LOGGED IN AS
Aaron Woland
aawoland@cisco.com
Profile

Sign Out

ORGANIZATION SELECTED
genie
readonly

Theme Light Dark

Integration Status

10 Providers Synced

Last data collection

Providers

Demo AWS
Success
Average Traffic: 26 records

Demo Auth0
Success
Average Traffic: 45 records

Demo Azure AD
Success
Average Traffic: 25 records

Demo Duo
Success
Average Traffic: 59 records

Demo GSuite
Success
Average Traffic: 65 records

Demo GitHub
Success
Average Traffic: 19 records

Demo Okta
Success
Average Traffic: 133 records

Demo Salesforce
Success
Average Traffic: 44 records

Demo Workday
Success
Average Traffic: 43 records

Slack - oort-teamdata-testing
Success
Average Traffic: 10 records

Ticketin

Notification Targets

Okta Workflow

oort-demo

Identities

238
Total

234
In Protected Population

13
Inconsistent Users

MFA Status

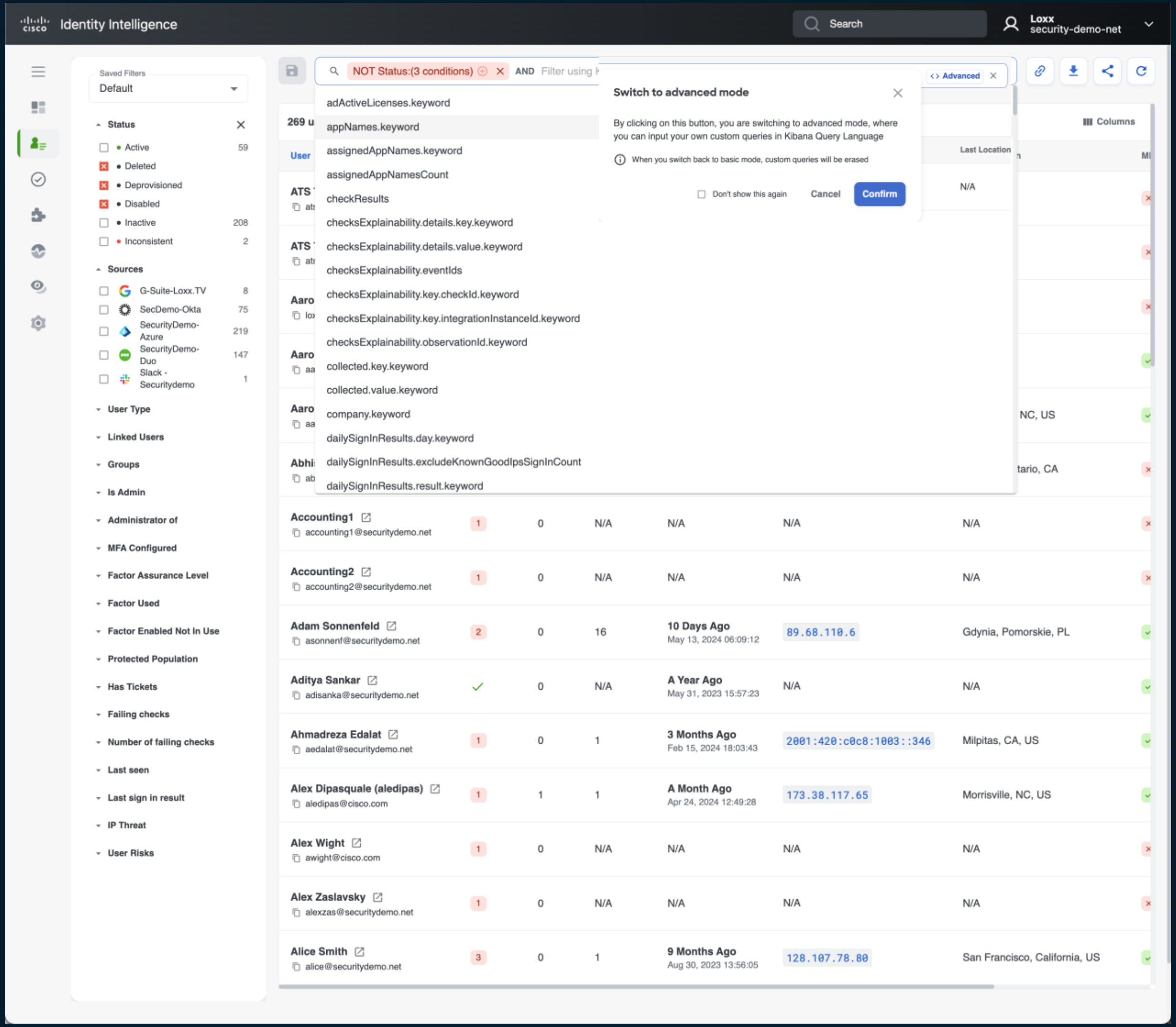
159
No MFA Configured

21
No Strong MFA Configured

22
Weak MFA Was Used To Successfully Sign In

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



Identity Intelligence

Search

Loxx
security-demo-net

Saved Filters
Default

Status
- ☐ Active 59
- ☒ Deleted
- ☒ Deprovisioned
- ☒ Disabled
- ☐ Inactive 208
- ☐ Inconsistent 2

Sources
- ☐ G-Suite-Loxx.TV 8
- ☐ SecDemo-Okta 75
- ☐ SecurityDemo-Azure 219
- ☐ SecurityDemo-Duo 147
- ☐ Slack - Securitydemo 1

User Type
Linked Users
Groups
Is Admin
Administrator of
MFA Configured
Factor Assurance Level
Factor Used
Factor Enabled Not In Use
Protected Population
Has Tickets
Failing checks
Number of failing checks
Last seen
Last sign in result
IP Threat
User Risks

NOT Status:(3 conditions) AND Filter using

<> Advanced

- adActiveLicenses.keyword
- appNames.keyword
- assignedAppNames.keyword
- assignedAppNamesCount
- checkResults
- checksExplainability.details.key.keyword
- checksExplainability.details.value.keyword
- checksExplainability.eventIds
- checksExplainability.key.checkId.keyword
- checksExplainability.key.integrationInstanceId.keyword
- checksExplainability.observationId.keyword
- collected.key.keyword
- collected.value.keyword
- company.keyword
- dailySignInResults.day.keyword
- dailySignInResults.excludeKnownGoodIpsSignInCount
- dailySignInResults.result.keyword

Switch to advanced mode

By clicking on this button, you are switching to advanced mode, where you can input your own custom queries in Kibana Query Language

When you switch back to basic mode, custom queries will be erased

☐ Don't show this again   Cancel   Confirm

269 u

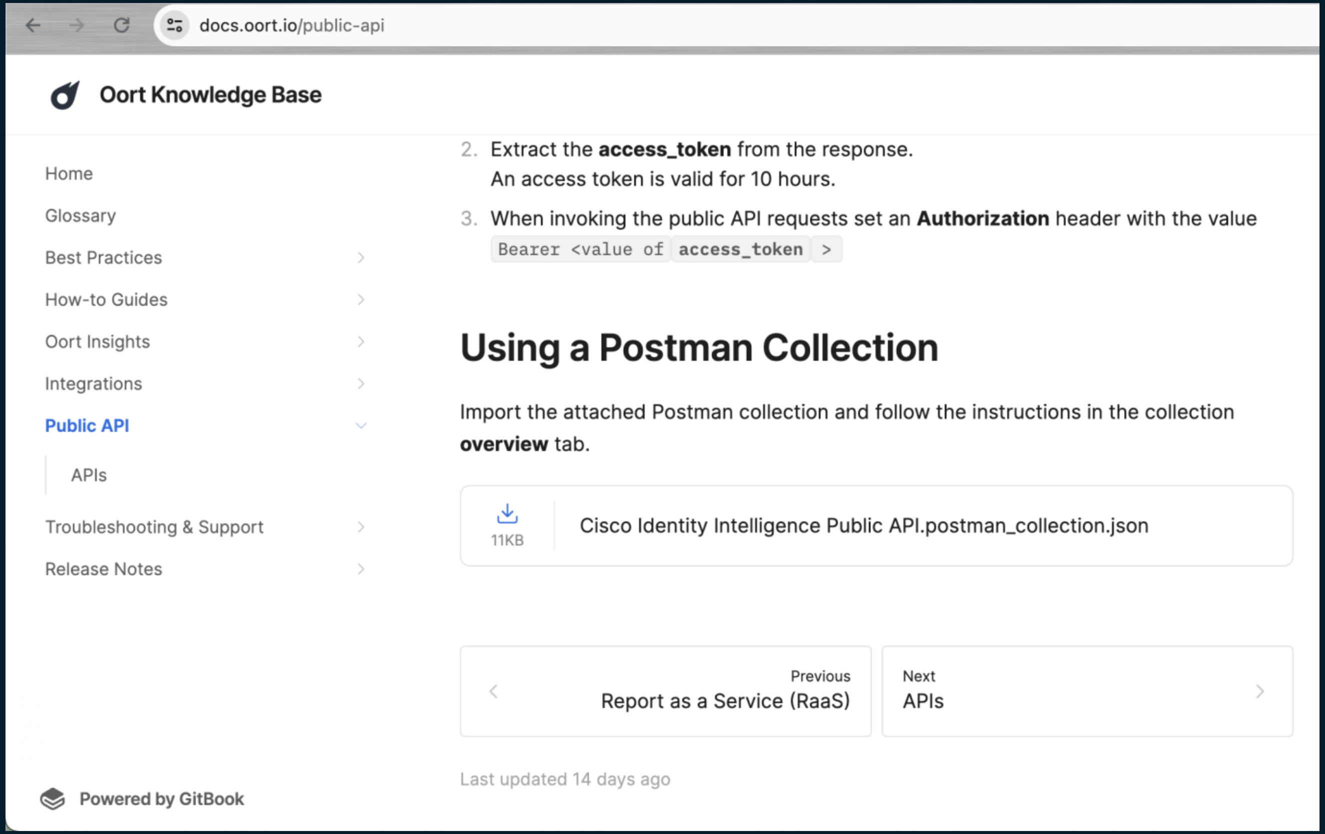
Columns

User						Last Location	MI
Accounting1 accounting1@securitydemo.net	1	0	N/A	N/A	N/A	N/A	✗
Accounting2 accounting2@securitydemo.net	1	0	N/A	N/A	N/A	N/A	✗
Adam Sonnenfeld asonnenf@securitydemo.net	2	0	16	10 Days Ago May 13, 2024 06:09:12	89.68.110.6	Gdynia, Pomorskie, PL	✓
Aditya Sankar adisanka@securitydemo.net	✓	0	N/A	A Year Ago May 31, 2023 15:57:23	N/A	N/A	✓
Ahmadreza Edalat aedalat@securitydemo.net	1	0	1	3 Months Ago Feb 15, 2024 18:03:43	2001:420:c0c8:1003::346	Milpitas, CA, US	✓
Alex Dipasquale (aledipas) aledipas@cisco.com	1	1	1	A Month Ago Apr 24, 2024 12:49:28	173.38.117.65	Morrisville, NC, US	✓
Alex Wight awight@cisco.com	1	0	N/A	N/A	N/A	N/A	✗
Alex Zaslavsky alexzas@securitydemo.net	1	0	N/A	N/A	N/A	N/A	✗
Alice Smith alice@securitydemo.net	3	0	1	9 Months Ago Aug 30, 2023 13:56:05	128.107.78.80	San Francisco, California, US	✓

Let’s talk about APIs

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



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

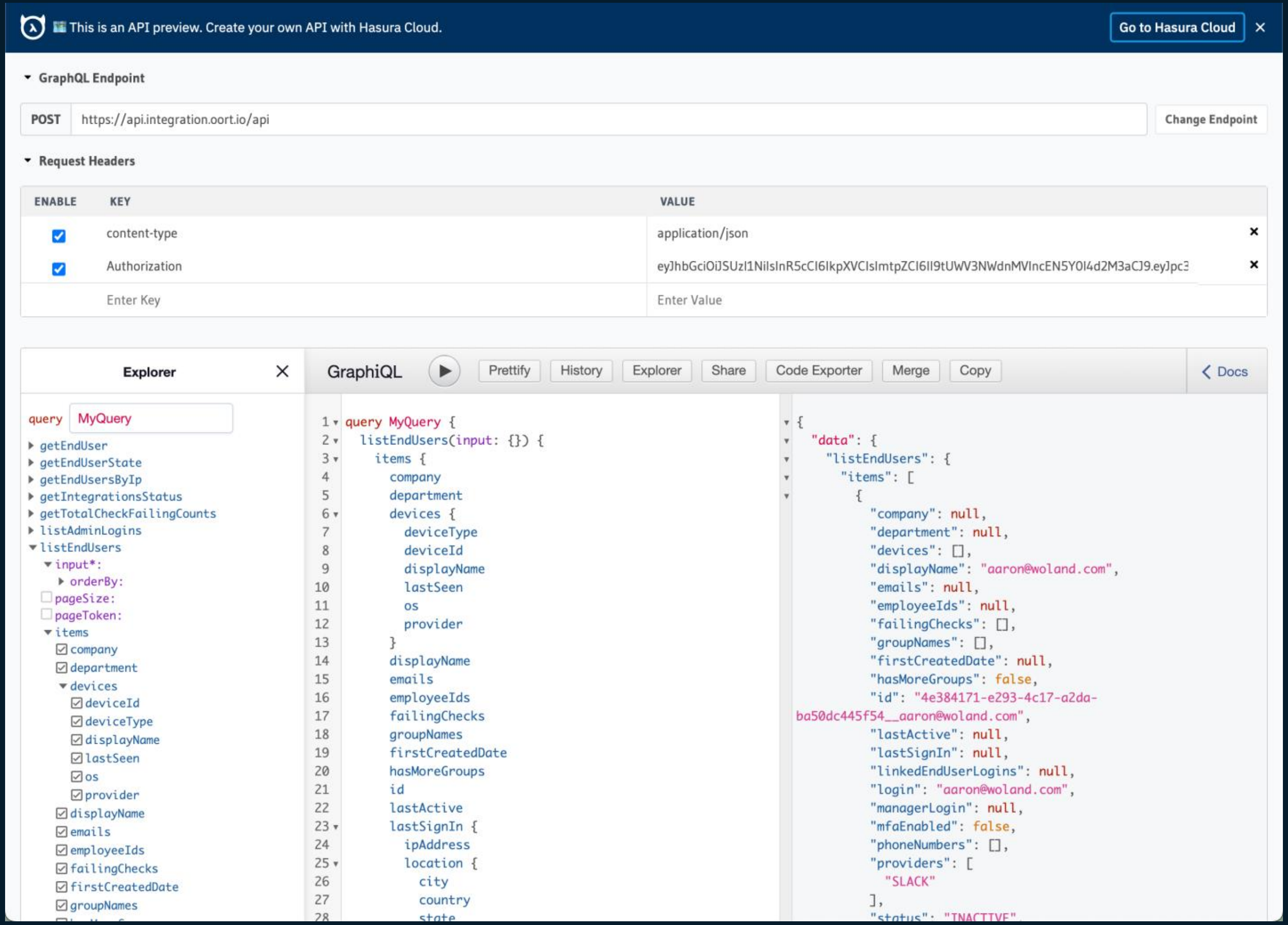
Previous Report as a Service (RaaS)

Next APIs

Last updated 14 days ago

GraphQL Explorer Tools

- Hasura GraphQL Explorer
  - Wraps around the open_source GraphiQL 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/graphiql?endpoint=[INSERT_URL]



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

▾ GraphQL Endpoint

POST https://api.integration.oort.io/api

▾ Request Headers

ENABLE	KEY	VALUE
☑	content-type	application/json
☑	Authorization	eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Il9tUWV3NWdnMVIncEN5Y0l4d2M3aCJ9.eyJpc3
	Enter Key	Enter Value

query MyQuery

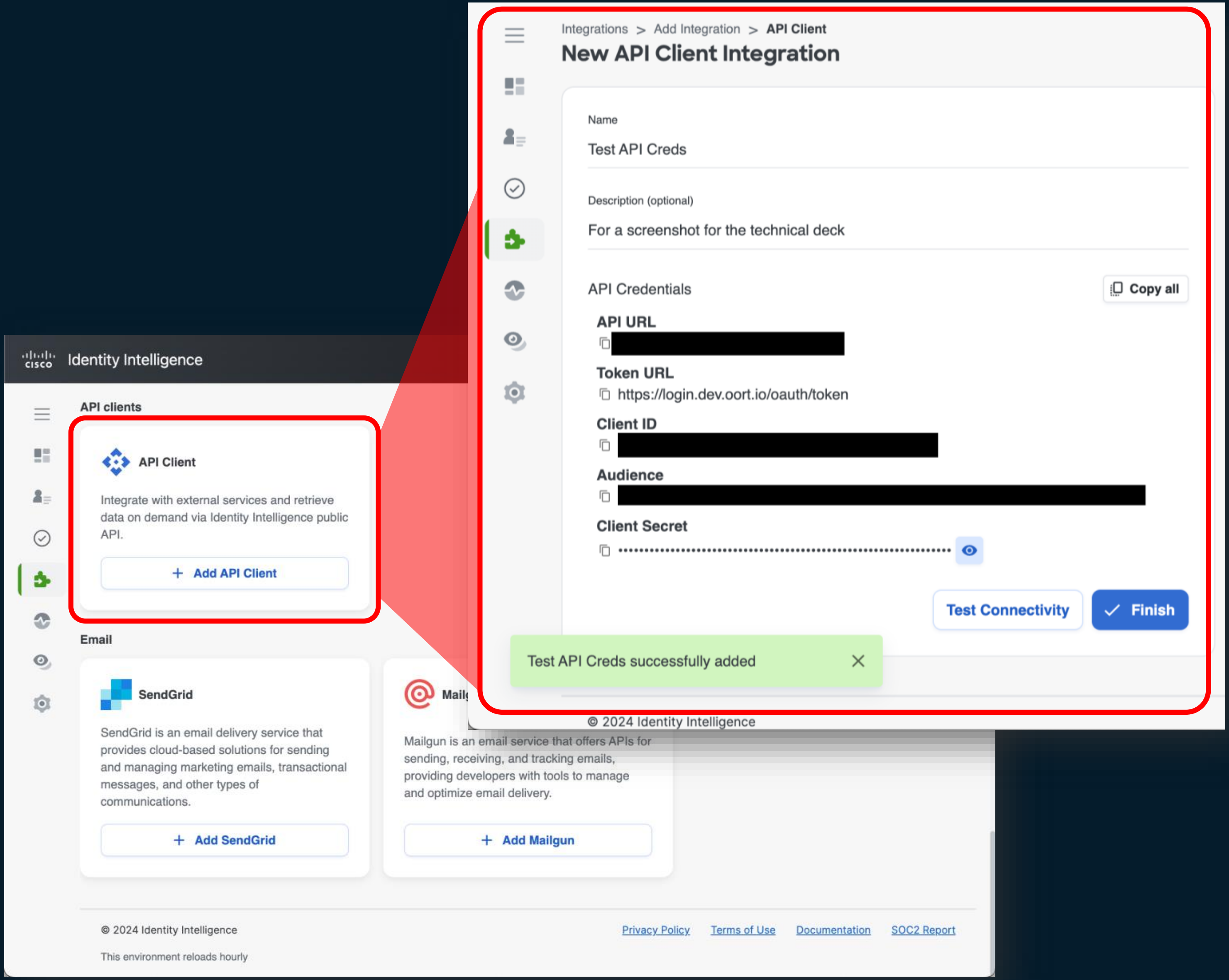
- ▸ getEndUser
- ▸ getEndUserState
- ▸ getEndUsersByIp
- ▸ getIntegrationsStatus
- ▸ getTotalCheckFailingCounts
- ▸ listAdminLogins
- ▾ listEndUsers
  - ▾ input*:
    - ▸ orderBy:
  - □ pageSize:
  - □ pageToken:
  - ▾ items
    - ☑ company
    - ☑ department
    - ▾ devices
      - ☑ deviceId
      - ☑ deviceType
      - ☑ displayName
      - ☑ lastSeen
      - ☑ os
      - ☑ provider
    - ☑ displayName
    - ☑ emails
    - ☑ employeeIds
    - ☑ failingChecks
    - ☑ firstCreatedDate
    - ☑ groupNames

```
query MyQuery {
  listEndUsers(input: {}) {
    items {
      company
      department
      devices {
        deviceType
        deviceId
        displayName
        lastSeen
        os
        provider
      }
      displayName
      emails
      employeeIds
      failingChecks
      groupNames
      firstCreatedDate
      hasMoreGroups
      id
      lastActive
      lastSignIn {
        ipAddress
        location {
          city
          country
          state
```

```
{
  "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"
          ],
          "status": "INACTIVE",
```

Create API Key(s)

- In the “integrations” section of the UI
  - Add a new API Client
  - Generates the API ClientID/Secret pair to get a bearer token



Identity Intelligence

API clients

API Client

Integrate with external services and retrieve data on demand via Identity Intelligence public API.

+ Add API Client

Email

SendGrid

SendGrid is an email delivery service that provides cloud-based solutions for sending and managing marketing emails, transactional messages, and other types of communications.

+ Add SendGrid

Mail

Mailgun is an email service that offers APIs for sending, receiving, and tracking emails, providing developers with tools to manage and optimize email delivery.

+ Add Mailgun

© 2024 Identity Intelligence

This environment reloads hourly

Privacy Policy Terms of Use Documentation SOC2 Report

Integrations > Add Integration > API Client

New API Client Integration

Name

Test API Creds

Description (optional)

For a screenshot for the technical deck

API Credentials

Copy all

API URL

[redacted]

Token URL

https://login.dev.oort.io/oauth/token

Client ID

[redacted]

Audience

[redacted]

Client Secret

••

Test Connectivity

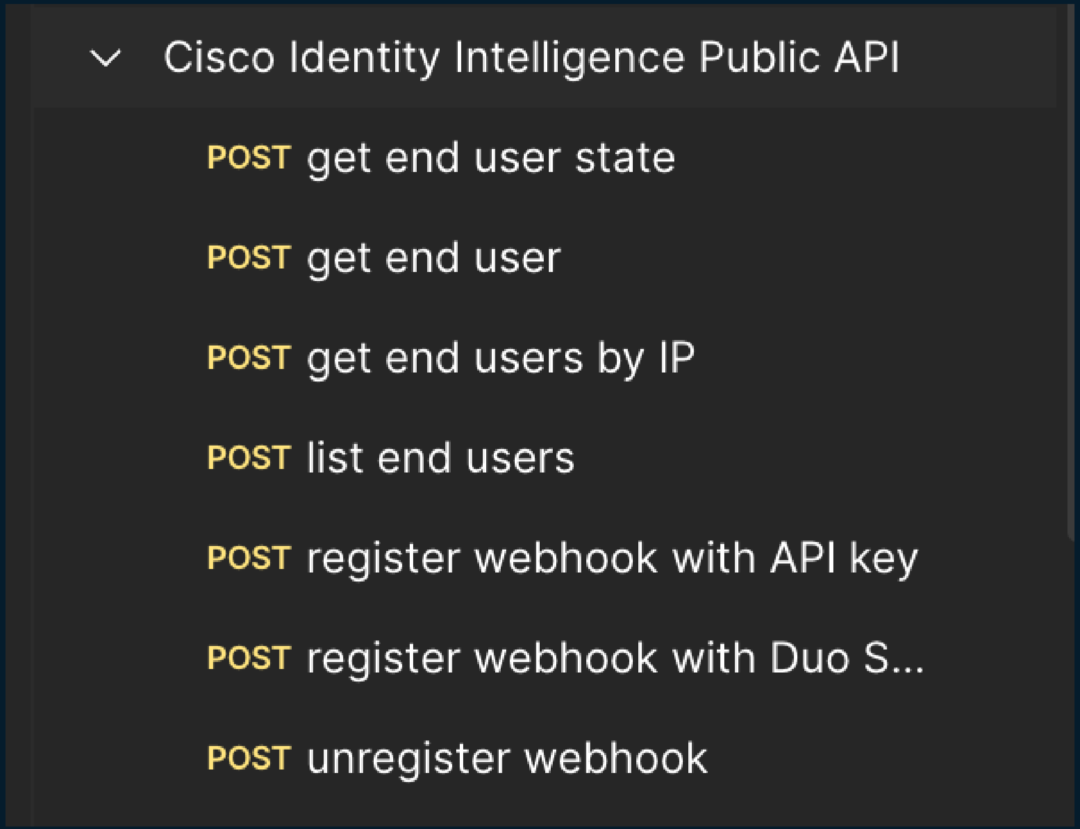
✓ Finish

Test API Creds successfully added ✕

© 2024 Identity Intelligence

Query’s Available via Public API

- list end users – bulk response with key attributes of the digest
- get end user state – gets partial digest for specific user
- get end user – retrieves the full context of a user
- get end users by IP – all users that are associated with an IP



Cisco Identity Intelligence Public API

POST get end user state

POST get end user

POST get end users by IP

POST list end users

POST register webhook with API key

POST register webhook with Duo S...

POST unregister webhook

Call to Action

- Login to the Genie demo tenant & get a feel for Identity Intelligence
  - https://dashboard.stage.oort.io/ > Login > type “Genie” in the tenant name
- Provision your own CII tenant from Duo, if you have Advantage or Above
- Didi & Lital Show (Oort’s CTO has his own podcast) https://www.youtube.com/@thedidilitalshow

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

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

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer 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

Contact me using Webex messaging

The bridge to possible

Thank you

#CiscoLive