Air Force Mobile Connect

Driving Zero Trust and Extending Capability

Capt George Calley, James Crocker,
Rob Gordon, Dave Zukowski

29 August 2023

CLOUD ONE
FAST
SECURE
STREAMLINED

Introductions

CLOUD ONE
FAST SECURE STREAMLINED

At A Glance

June 2023

168
Systems Hosted

Systems Live in C1 Production

AWS 68

Azure 41

Akamai 4

320
**Total Systems In-Flight

140
ATOS Granted

*Includes C1 Zone C workloads
**Includes DE projects

DEFENDED

Attacks Prevented Last Month	SQL Injection	Cross-site Scripting	HTTP Anomaly	Command Injection	PHP Injection	Remote File Inclusion
657,407	154,645	269,059	1,244	220,262	6,621	5,576

DEPLOYED

DEPLOYMENT ARTIFACTS
4,942,504

AWS	AZURE
4,829,744	112,760

TOTAL DATA STORED/HOSTED
24,509 TB

AWS	AZURE
20,508 TB	4,001 TB Data Services App *1,417 TB by itself

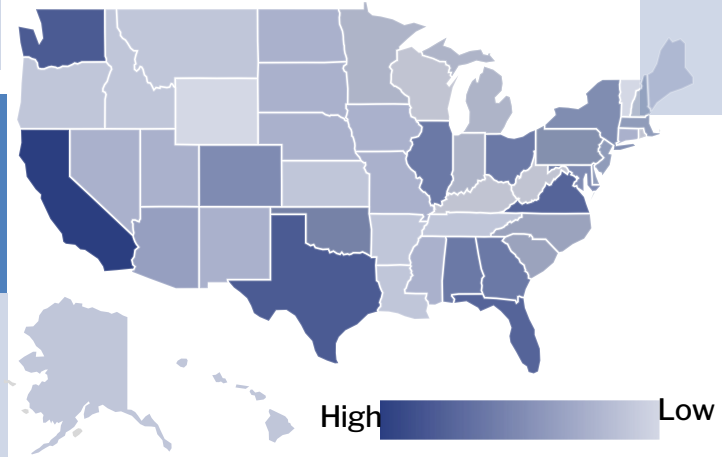
DELIVERED

SMTP Messages Sent Per Week
470 K

MONTHLY LOGINS
19,943,678

WEEKLY AVG.	DAILY AVG.
5M	665K

Requests By State



*Requests By Country Per Week

1. U.S.A.	361,724,679
2. Germany	3,380,139
3. Japan	2,734,558
4. Great Britain	2,179,119
5. Italy	1,324,684
6. South Korea	667,995
7. Qatar	363,918
8. Puerto Rico	331749

OPTIMIZED

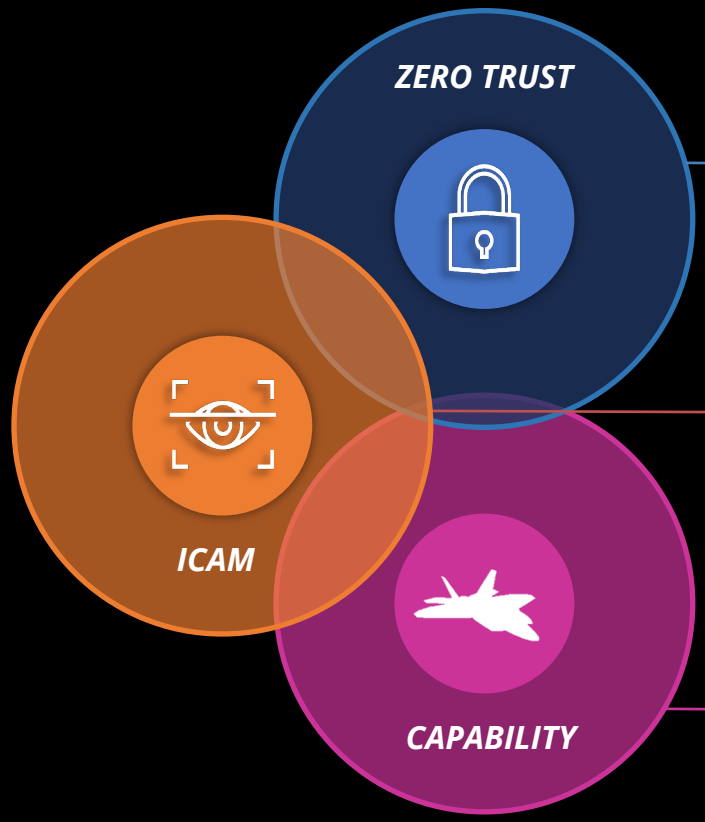
HITS PER SECOND (PEAK)
595

	Traffic Offloaded
NIPRNet 366	34%
Commercial 230	30%

AVG. WEEKLY THROUGHPUT
55.35 TB

	Data Offloaded
NIPRNet 46.15 TB	41%
Commercial 9.2 TB	34%

Zero Trust Journey



KEY CROSS-CAPABILITY ELEMENTS

- SASE integration to enable continuous authentication, macro-segmentation security functions
- Continuous logging and inspection of traffic
- Policy enforcement on every transaction

- **Use credentials that comply with NIST 800.64**
- **Context aware authentication**
- **IAL/AAL inform AuthN and AuthZ decistions**

- **Enhance capability**
- **Expand access options**
- **Prioritize user experience**

Use Case

- Non-CAC devices
- Non-CAC eligible community

What is MobileConnect AF?

- Evolved out of partnership with Army
- Extended partnership with BESPIN
- Offered as a C1 common service - extension of ICAM offerings
- Built on top of C1 Enterprise ICAM services that process >40 Million monthly logins & perform > 1B authz requests annually
- Available on iOS and Android app stores as a free app for BYOD devices
- Registration available at mobileconnect.cce.af.mil

MobileConnect Components & Roadmap

Live now (USAF & Army)

- Registration Application (mobileconnect.cce.af.mil)
- Mobile Application (iOS / Android)
- SSO Configuration Application (GCDS Portal)
- Back-end SSO services (integration with USAF & Army Identity Stores, multiple protocol support)
- Full integration with Policy Engine / Policy Enforcement

In Beta Testing Now (Live for Army)

- Sponsorship Application (for sponsoring non-CAC holders)

In Alpha Testing Now

- HW Token-based passkey integration (Yubikey)

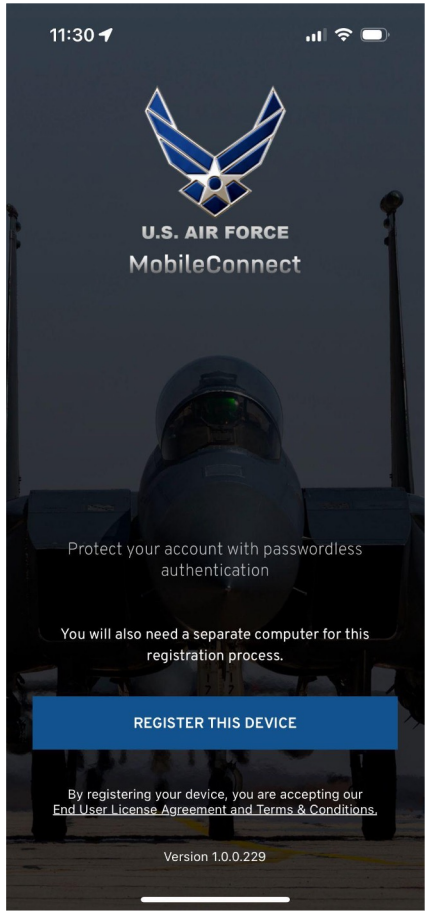
Roadmap (Next 6 months)

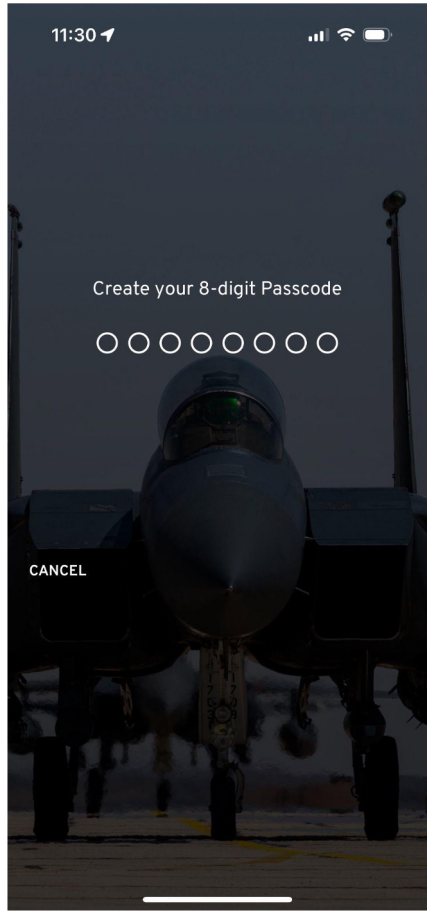
- Mobile SDK - supporting native SSO capabilities to USAF-developed Mobile Applications

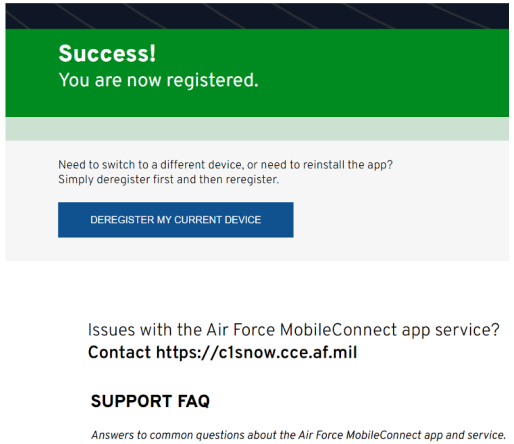
MobileConnect - Registration

MobileConnect registration is available to all existing Cloud One users.

- In a browser go to [MobileConnect site] and select ‘Register’
- Download the MobileConnect USAF application from the Google or Apple app store and Register the device by scanning the QR code
- Set an 8-digit PIN for the device.





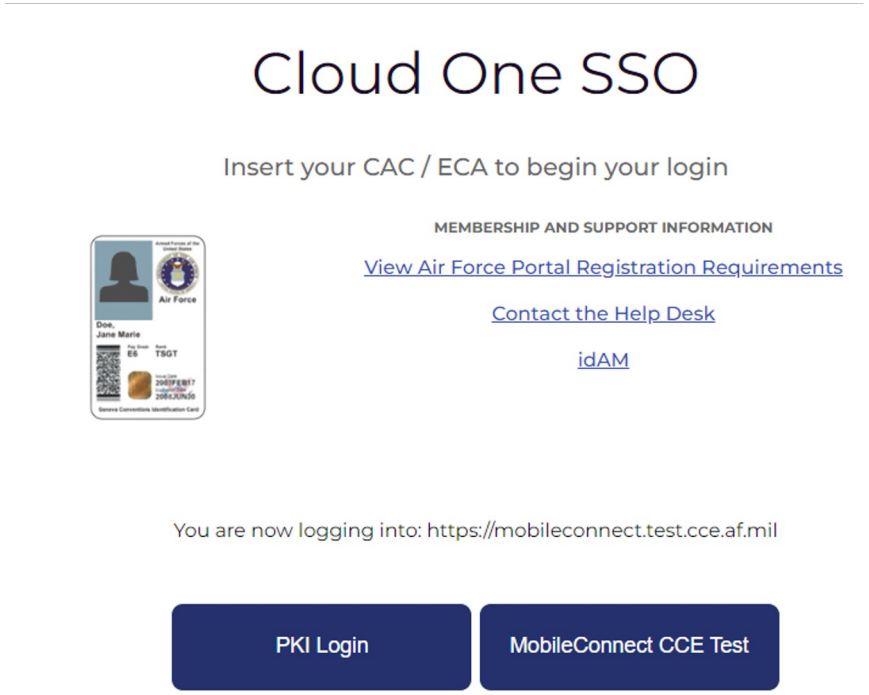


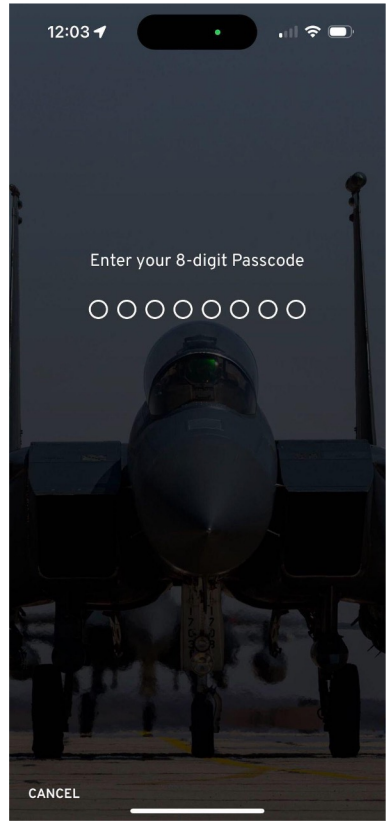
Issues with the Air Force MobileConnect app service?
Contact https://c1snow.cce.af.mil

SUPPORT FAQ

Answers to common questions about the Air Force MobileConnect app and service.

MobileConnect - Primary Factor Login

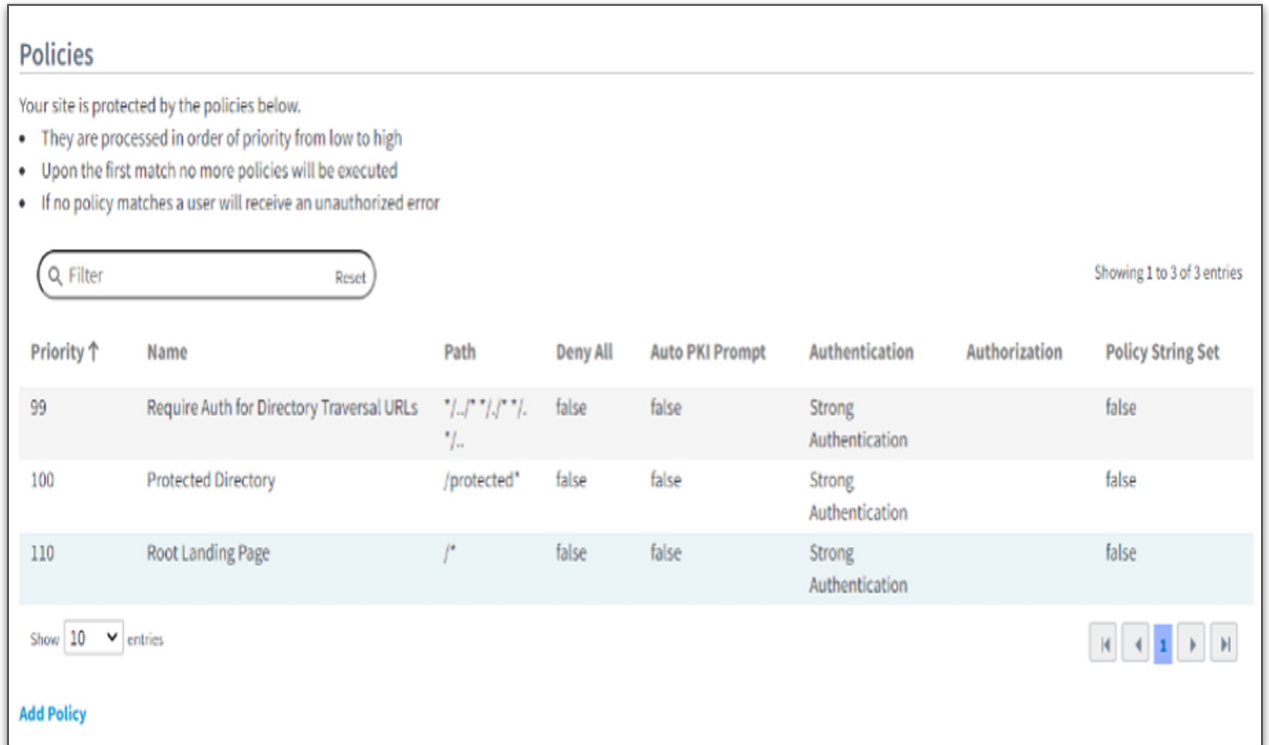


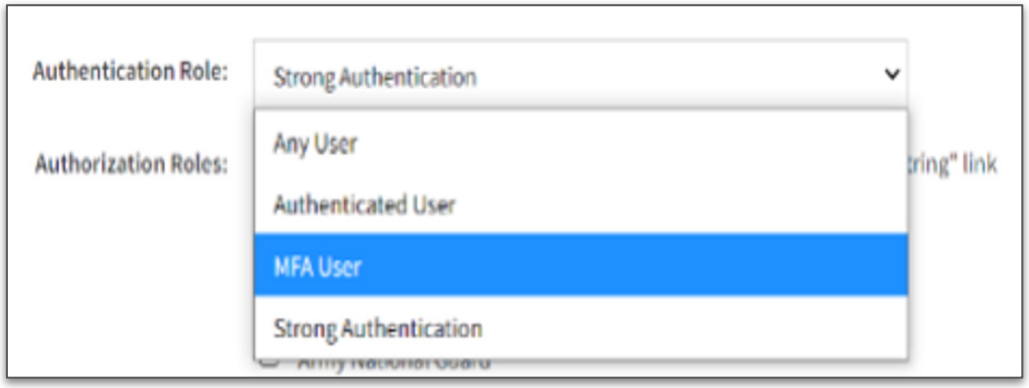


Applications that are enabled with MobileConnect Login will present as second authentication option on the login screen. Users simply click the button, scan the QR code, and enter their PIN and they are logged in successfully

MobileConnect - SSO Configuration

- Within the GCDS Portal (https://control.akamai.csd.disa.mil) application owners are able to configure their sites to require MFA.
- During policy setup, selecting the authentication role will determine what is required by the user when accessing certain paths.
  - Any User = not authentication required
  - Authenticated User = username/password required (Not used by USAF Currently
  - MFA User = MobileConnect Primary Factor
  - Strong Authentication = Must login with CAC





USAF SSO Reporting & Monitoring

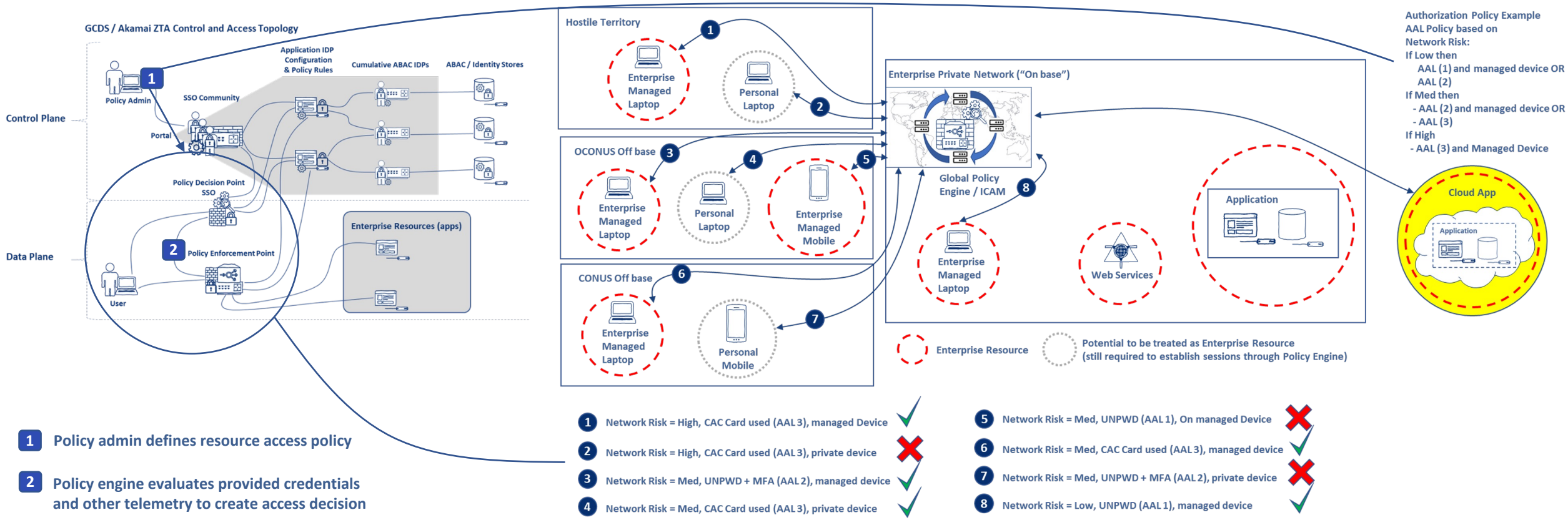
MobileConnect is integrated with GCDS's enterprise SSO offering, providing sortable / filterable / reportable statistics on successful / failed authentication attempts that are accessible to Mission Application owners

Cloud One Policy Engine - Overview

Cloud One's Policy engine provides a suite of capabilities to Cloud One customers. Key Features include:

- **Highly Scalable, Resilient, and Performant - currently processing > 1 Billion Authorization events annually**
- **Globally distributed in over 30 discrete locations, both CONUS and OCONUS. Presence on both unclassified and classified networks**
- **Provides the ability to define custom authorization policies that restrict content based on ANY combination of available attributes (including authenticator)**
- **Can evaluate multiple policies in a configurable order, providing infinite flexibility in authorization rules**
- **Able to restrict content by authentication type - down to the individual path or even resource/document**
- **Policies are evaluated on every request - at the GCDS edge, allowing for extreme scalability**
- **Support for all SSO Property types (including SAML, ADFS and OIDC)**
- **Solution is entirely managed through configuration via the GCDS portal, allowing for changes to be made quickly and easily (changes propagate in approx 5 minutes), but with full audit traceability**

GCDS Policy Engine - Architecture



1. Policy admin defines resource access policy
2. Policy engine evaluates provided credentials and other telemetry to create access decision

1. Network Risk = High, CAC Card used (AAL 3), managed Device ✓
2. Network Risk = High, CAC Card used (AAL 3), private device ✗
3. Network Risk = Med, UNPWD + MFA (AAL 2), managed device ✓
4. Network Risk = Med, CAC Card used (AAL 3), private device ✓
5. Network Risk = Med, UNPWD (AAL 1), On managed Device ✗
6. Network Risk = Med, CAC Card used (AAL 3), managed device ✓
7. Network Risk = Med, UNPWD + MFA (AAL 2), private device ✗
8. Network Risk = Low, UNPWD (AAL 1), managed device ✓

This is a core and critical part to the basic architectural framework of Cloud One. Cloud One only allows communication to the resources it hosts by communication paths defined by the control plane and enabled through the policy engine.

GCDS Policy Engine - Key Concepts

The Policy Engine leverages the following feature sets that can be configured via the GCDS portal:

Attribute Mapping: GCDS SSO integrates with multiple back-end identity stores (C1 AAD, Army AMID, etc…) and allows administrators to configure the way attributes are mapped. These attributes can then be passed to applications or used for policy enforcement.

Authentication Roles: GCDS SSO enforces the identity and authentication assurance levels described in NIST 800-63, allowing roles to be created that correspond to credential strength and the level of identity proofing. This allows system owners to configure areas of their site that are publicly available, while restricting other areas to CAC or MFA - depending on system owner needs.

Authorization Roles: Any of the attributes provided by the identity store can be used to define authorization roles that can be applied to applications in order to restrict access. Need to restrict certain pages/paths to prevent Foreign National access or prevent contractors from accessing military-only content? Authorization rules can provide this capability in an easily configurable manner!

Policies: Combining the above concepts together, GCDS lets application administrators combine authentication and authorization roles into a series of policy statements that provide complete control over access to resources (down to the individual file/document level).

Attribute Customization

GCDS SSO integrates with any number of back-end identity stores (IDS) and allows application owners to configure the attributes they require - both for authorization and identity purposes.

Any attribute from the identity store can be configured as an authorization attribute

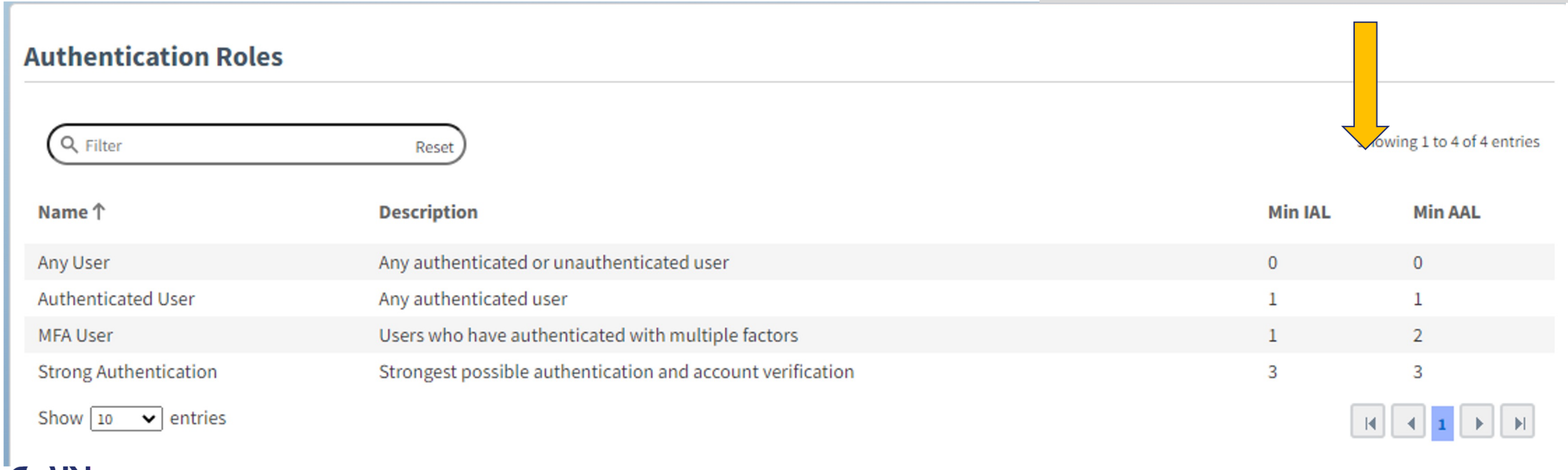
Name ↑	Display Name
aal	AUTHLEVEL
armyaccounttype	ARMYACCOUNTTYPE
armyaoc1	ARMYAOC1
armyaoc2	ARMYAOC2
armybabr	ARMYBABR
armybabrdesc	ARMYBABRDESC
armycaccn	ARMYCACCN
armyCity	ARMYCITY
armycompany	ARMYCOMPANY
armycomponent	ARMYCOMPONENT
armycountry	ARMYCOUNTRY
armycrfld1	ARMYCRFLD1
armycrfld2	ARMYCRFLD2
armydsn	ARMYDSN
armydymose	ARMYDYMOSE
armyedipi	ARMYEDIPI
armyeemail	ARMYEEMAIL
armyeuid	ARMYEUID
armyexternalmail	ARMYEXTERNALMAIL
armyfin	ARMYFIN
armygrade	ARMYGRADE
armymacom	ARMYMACOM
armymiddlename	ARMYMIDDLENAME

Attribute names can be mapped to alternate names to ensure that customers receive attributes that are named the way their applications need them to be!

Authentication Roles

GCDS SSO allows for authentication roles to be configured that automatically enforce Identity and Authentication Assurance Levels (IAL & AAL) as defined in NIST 800-63

Roles can be defined that specify the minimum required level of identity proofing, and the minimum allowed credential strength. These roles can be applied to applications, paths, or individual documents/resources!



Authorization Roles

Any combination of attributes can be configured as a custom role. Roles can be applied to applications, paths, or individual resources to restrict access at the GCDS edge.

Roles can be shared / re-used across multiple systems / portfolios as long as they retrieve their attributes from the same identity store

Roles can be used to restrict content by rank, branch, CTR/CIV/MIL, or any other attribute that is available in the identity store

Any combination of attributes can be assembled into a role using simple expression statements

Policy Engine Configuration

Policies

Your site is protect
- They are proces
- Upon the first r
- If no policy mat

Applications can have multiple policies configured, and they are evaluated in priority order on EVERY request - allowing for complete control of who has access to what!

Policy rules can be applied to paths, individual resources, or an entire application

Resources can also be set to require a minimum login assurance level (CAC only, MFA, public content etc…). GCDS will prompt for a 'session upgrade' when needed

Filter Reset

Showing 1 to 3 of 3 entries

Priority ↑	Name	Path	Deny All	Auto PKI Prompt	Authentication	Authorization	Policy String Set
100	Block Contractor Access	/epubs/DR_pubs/DR_b/*	false	false	Strong Authentication		true
200	PKI User including CTR (block Foreign)	/Tools/Videos/*	false	false	MFA User		true
500	Any User	/*	false	false	Any User		false

Show 10 entries

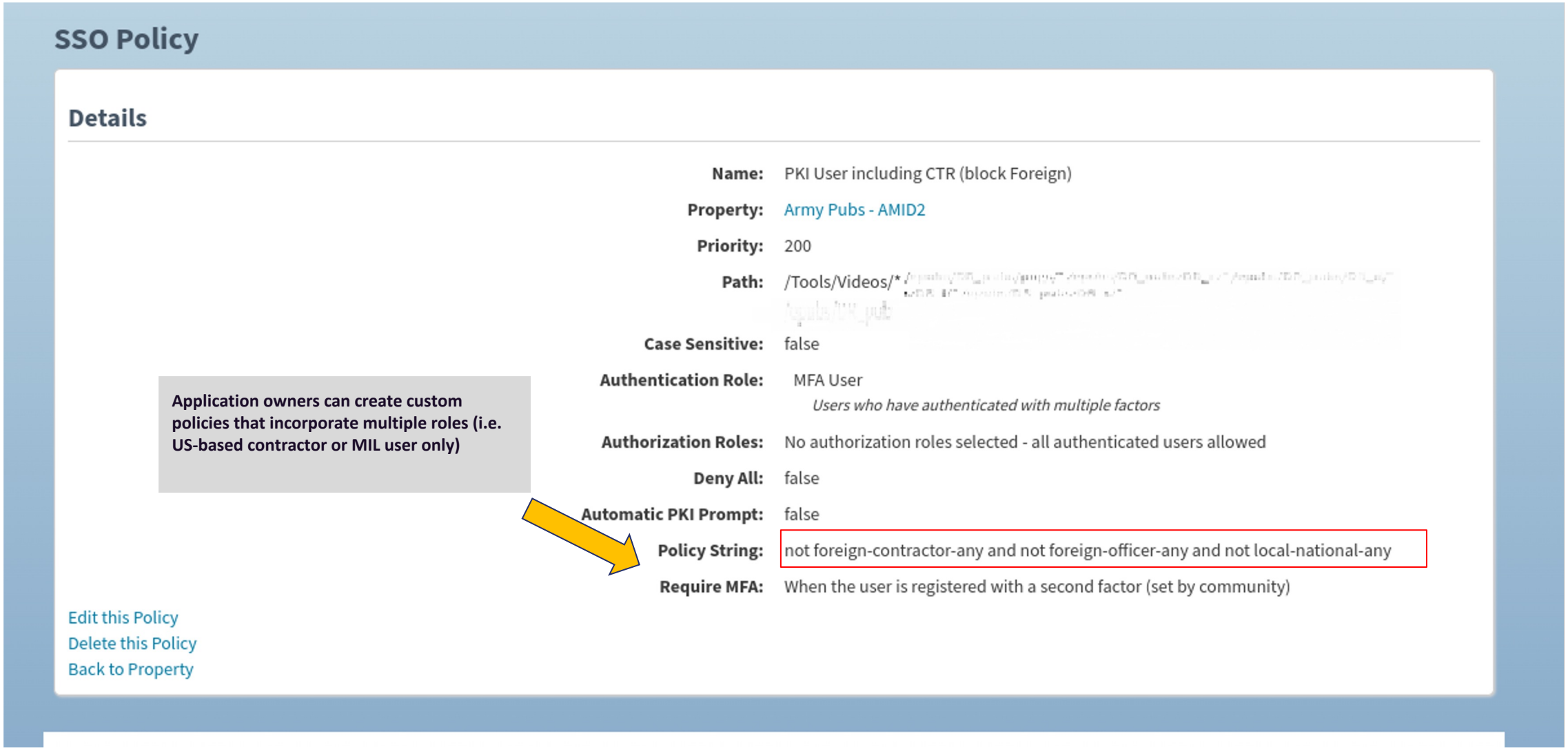
1

Add Policy

Policy strings determine the attribute logic that is applied for each rule (the combination of Authorization Rules)

Custom Policies

Authorization Policies are used to define rules involving one or more role. The following example shows how a 'foreign national block' can be defined.



Application owners can create custom policies that incorporate multiple roles (i.e. US-based contractor or MIL user only)

Policy Engine In Action: Demo

Cloud One Example - JCaaS

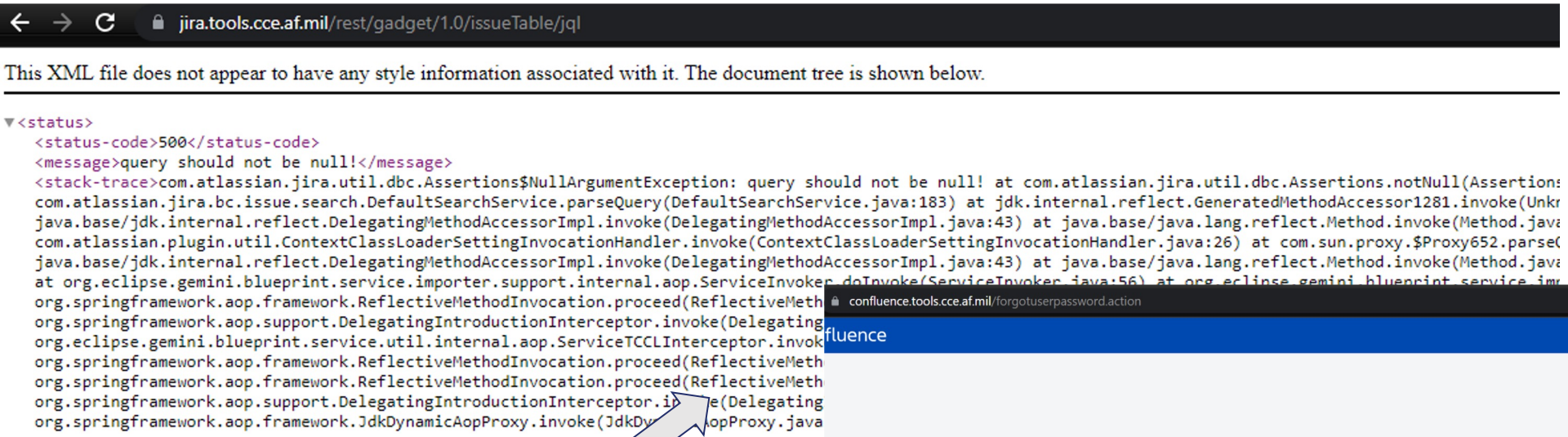
Cloud One WAF is constantly alerting on unauthorized / unauthenticated users scanning publicly accessible areas of Jira and Confluence - looking for information on how the system is configured

Response status code of 200 indicates that the (unauthenticated) user was able to successfully interact with the API / resource

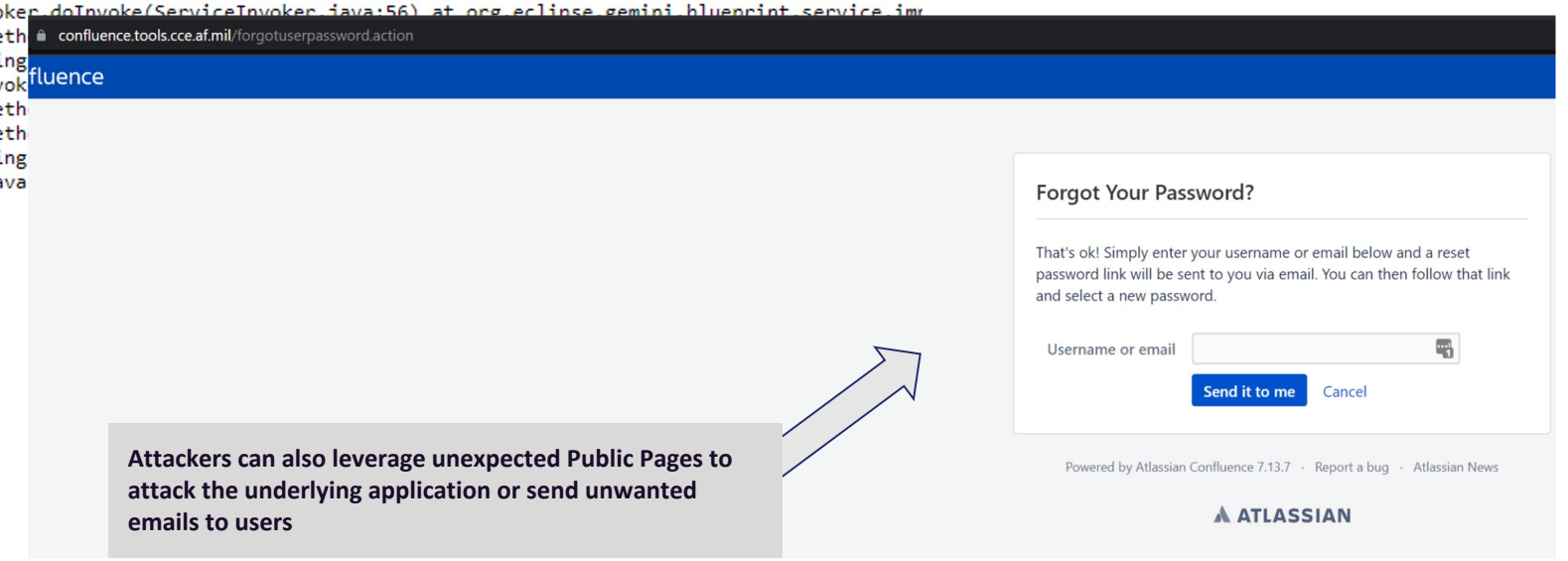
Hostname	Path	Status	Action Applied
confluence.tools.cce.af.mil	/rest/mywork/latest/status/notification/count	200	Alert
jira.tools.cce.af.mil	/rest/menu/latest/appswitcher	200	Alert
jira.tools.cce.af.mil	/rest/greenhopper/1.0/xboard/work/allData.json	200	Alert
jira.tools.cce.af.mil	/rest/greenhopper/1.0/xboard/work/69/colors.json	200	Alert
jira.tools.cce.af.mil	/rest/greenhopper/1.0/xboard/issue/details.json	200	Alert
jira.tools.cce.af.mil	/rest/gadget/1.0/issueTable/jql	200	Alert
jira.tools.cce.af.mil	/rest/gadget/1.0/issueTable/jql	200	Alert
jira.tools.cce.af.mil	/rest/gadget/1.0/issueTable/jql	200	Alert
confluence.tools.cce.af.mil	/rest/dashboardmacros/1.0/updates	200	Alert
confluence.tools.cce.af.mil	/rest/api/search	200	Alert
confluence.tools.cce.af.mil	/rest/api/search	200	Alert

Cloud One Example - JCaaS

By default, JIRA & Confluence provide a set of APIs & other features that are not behind authentication by default. Adversaries can scan these APIs to gain clues about the configuration, environment, and software versions used by Cloud One and use this information for future attacks.



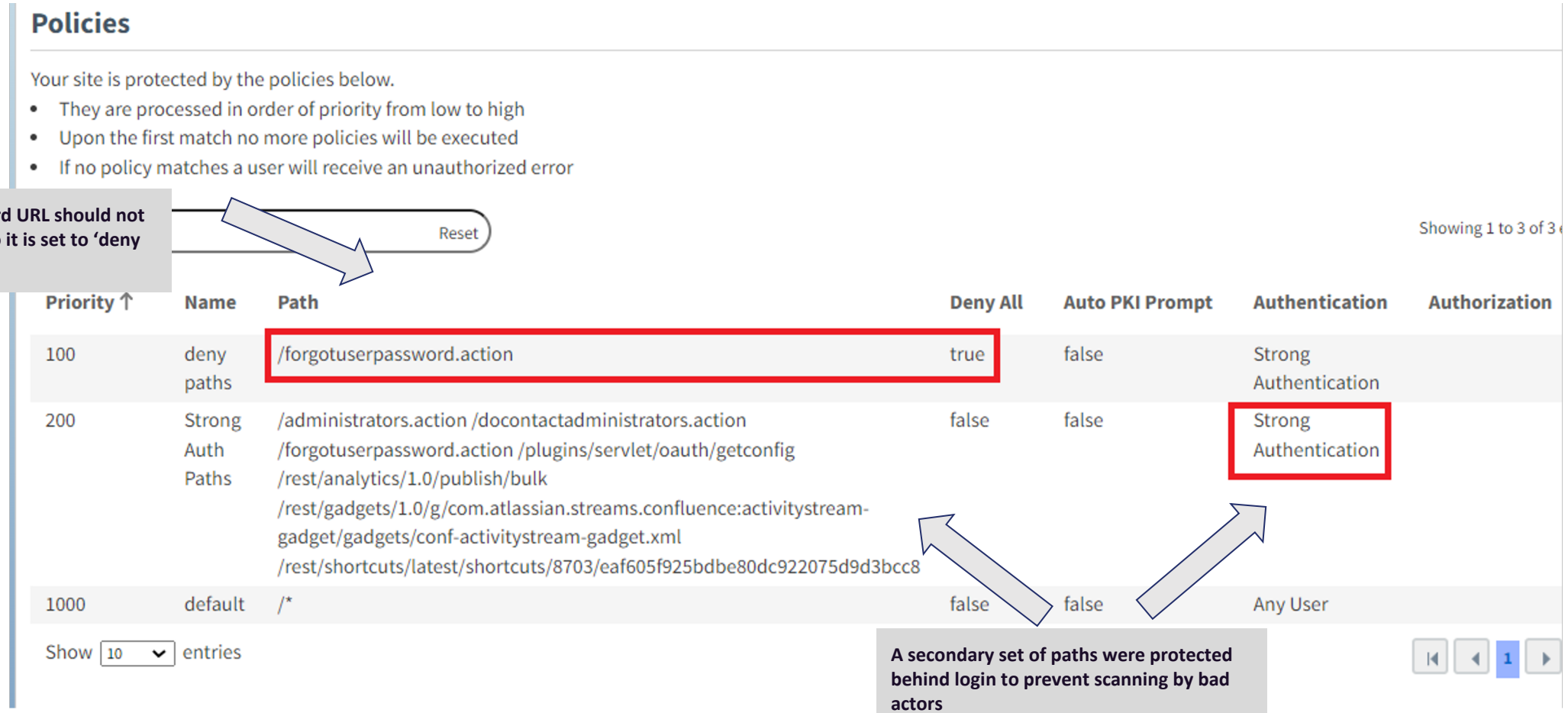
Attackers can glean information on environment configuration and underlying JAVA version by probing public API calls



Attackers can also leverage unexpected Public Pages to attack the underlying application or send unwanted emails to users

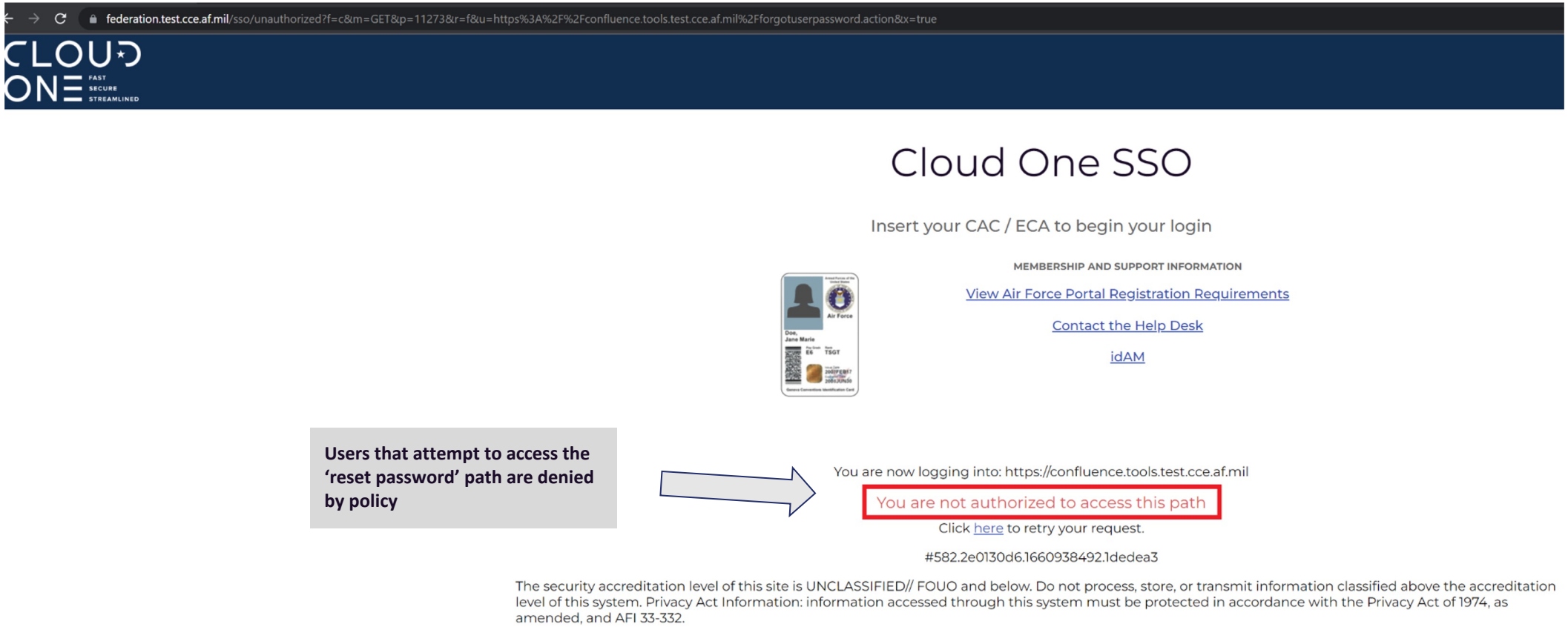
Cloud One Example - JCaaS - With Policy Engine

Applying a simple set of policies allowed the JCaaS team to quickly restrict access to pages that should not be accessible, and to enforce login requirements on pages that were previously open to scanning



Cloud One Example - JCaaS - Results

Applying a simple set of policies allowed the JCaaS team to quickly restrict access to pages that should not be accessible, and to enforce login requirements on pages that were previously open to scanning



MobileConnect support for Zero Trust: Logging

One of the key tenets of Zero Trust is to leverage all the data that you have at your disposal in order to continuously improve your authorization rule-sets. Cloud One has been continually adding new features (like the policy engine) and has taken strides to ensure these new capabilities also support this key tenet.

We have improved our logging capabilities to aggregate key information about each request into an easy to consume format that will help us:

- **Identify suspicious activity patterns across ALL Cloud One applications**
- **Refine access policies based on observed user activities**
- **Support forensic requests more rapidly and efficiently**
- **Allow system owners to better understand who us using their system**
- **Better integrate with SIEM solutions and other authorized data consumers**

Logging Enhancement Overview

The logging enhancements are built on top of the GCDS policy engine in order to ensure that for all policy-engine enabled applications, all data about the user and their interaction with protected application(s) is logged with all relevant telemetry data, including:

- **Basic Request data (host, path, method, HTTP response code, etc…)**
- **User information (user ID, SSO session ID, IAL level)**
- **Authentication / Authorization data (authenticator type, AAL level, authentication / authorization status, relevant policy)**
- **Telemetry derived from GCDS (country, region, city)**

Logging Enhancement Example

STATUS	METHOD	HOST	PATH	USERID	LoginType	SessionId	IAL	AAL	AUTHN	AUTHZ	Action	POLICY	COMMUN	COUNTRY	REGION	CITY
302	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil/pub/cacsignin?resource=/pub						FALSE	TRUE	u	6582		JP	32	YOKOTA
200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil/pub/bin/getAllSubmittedForm	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil/pub/bin/getAllUserTasks?Aut	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil/pub/bin/getDashSubmittedFo	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil/pub/bin/notifyAllNewTasks?u	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil/pub/content/saffm/en.html	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil/pub/content/saffm/en/misce	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	6585	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil/pub/content/saffm/en/my-fo	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/pub/content/dam/catalogs/das	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/pub/content/dam/catalogs/das	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/pub/content/dam/catalogs/das	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/pub/content/dam/catalogs/das	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/pub/content/dam/catalogs/das	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/pub/content/dam/catalogs/das	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/pub/content/dam/catalogs/das	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA

All request data is logged. This allows for operators to record the exact sequence of requests in a user's session – even if it spans across multiple applications.

Information about the user is included with each log line, including their primary identifier, level of identity proofing (IAL), and their SSO session identifier (so traffic can be tied to a specific login event). This data is only present for logged-in users (which is why the 1st line in the example is blank).

The authenticator strength (AAL) and policy information is also logged, allowing operators to easily see whether or not a request was authenticated, whether or not the requesting user was authorized to the data they requests, and also WHY (by referring to the policy ID)

Geolocation data is appended to every request, allowing operators to determine the country, region, and city associated with each request

Logging Enhancement: Example (Data Exfil)

The following **hypothetical** example shows how the log data could be used to detect an authorized user performing suspicious activity (like crawling a site in order to scrape/exfiltrate documents / content)

STATUS	METHOD	HOST	PATH	USERID	LoginType	SessionId	IAL	AAL	AUTHN	AUTHZ	Action	POLICY	COMMUN	COUNTRY	REGION	CITY
302	GET	www.my.af.mil	/login						FALSE	TRUE	u	6582		US	VA	PETERSBURG
200	GET	www.my.af.mil	/docs/protected/0001.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	US	VA	PETERSBURG
200	GET	www.my.af.mil	/docs/protected/0002.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	US	VA	PETERSBURG
200	GET	www.my.af.mil	/docs/protected/0003.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	US	VA	PETERSBURG
200	GET	www.my.af.mil	/docs/protected/0004.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	US	VA	PETERSBURG
200	GET	www.my.af.mil	/docs/protected/0005.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	US	VA	PETERSBURG
403	GET	www.my.af.mil	/docs/restricted/0006.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	FALSE	f	3540	4	US	VA	PETERSBURG
403	GET	www.my.af.mil	/docs/restricted/0007.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	FALSE	f	3540	4	US	VA	PETERSBURG
403	GET	www.my.af.mil	/docs/restricted/0009.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	FALSE	f	3540	4	US	VA	PETERSBURG
404	GET	www.my.af.mil	/docs/restricted/0009.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	FALSE	f	3540	4	US	VA	PETERSBURG
404	GET	www.my.af.mil	/docs/protected/0010.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	US	VA	PETERSBURG
404	GET	www.my.af.mil	/docs/protected/0011.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	US	VA	PETERSBURG
404	GET	www.my.af.mil	/docs/protected/0012.html	INSIDER.THREAT.XXX	pki	c464fd1e-6be	3	3	TRUE	TRUE	p	3539	4	US	VA	PETERSBURG

Status Code shows which documents were successfully accessed and which were denied by policy. 404 responses can also indicate 'scanning' behavior (searching for valid documents to exfiltrate

Combining path and user info allows operators to detect a single user 'crawling' a site, looking for content in a variety of ways.

Attempts to access content that the user is not entitled to view are warning signs that can be flagged on

The policy that was evaluated and denied can provide additional key information. For example, if POLICY 3539 = Any DoD CAC holder, and POLICY 3540 = US-Citizens only, we can deduce information about the individual performing the scan

Logging Enhancement: User / Session Compromise

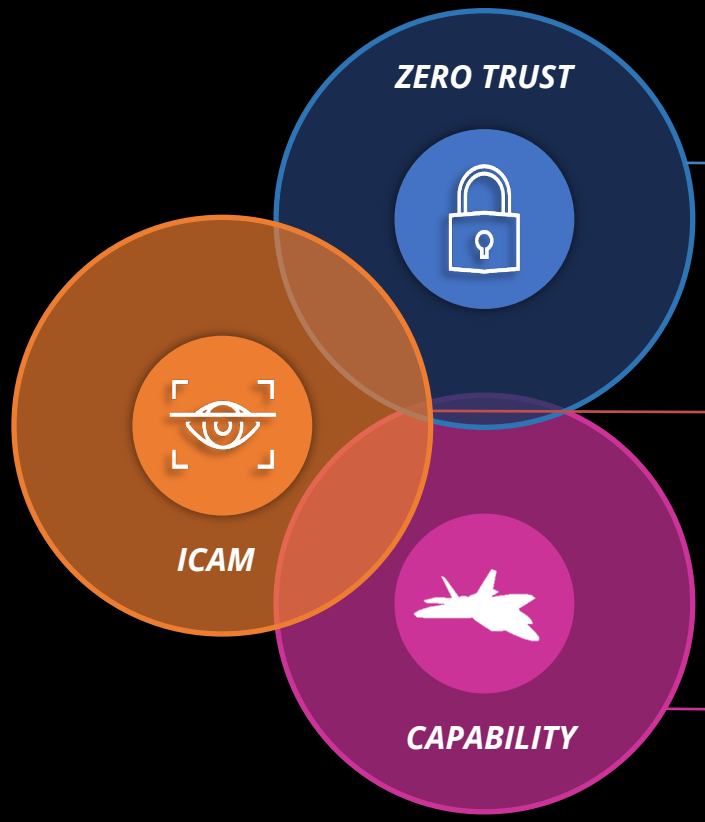
The following **hypothetical** example shows how the log data could be used to detect a user that has had their session / credentials compromised by a malicious actor

TIMESTAMP	STATUS	METHOD	HOST	PATH	USERID	LoginType	SessionId	IAL	AAL	AUTHN	AUTHZ	Action	POLICY	COMMUN	COUNTRY	REGION	CITY
1684520169	302	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil						FALSE	TRUE	u	6582		JP	32	YOKOTA
1684520170	200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520171	200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520172	200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520173	200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520174	200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520175	200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	6585	4	JP	32	YOKOTA
1684520176	200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520177	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520178	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520179	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520180	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520181	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520182	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	c464fd1e-6be7-4e6	3	3	TRUE	TRUE	p	3539	4	JP	32	YOKOTA
1684520173	302	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil						FALSE	TRUE	u	6582		US	AL	HUNTSVILLE
1684520174	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520175	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520176	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520177	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520178	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520179	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520180	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520181	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520182	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	3539	4	US	AL	HUNTSVILLE
1684520183	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	6585	4	US	AL	HUNTSVILLE
1684520184	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	6585	4	US	AL	HUNTSVILLE
1684520185	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	6585	4	US	AL	HUNTSVILLE
1684520186	200	GET	fams.cce.af.mil	/L/1/301843/1d/fams.cce.af.mil/	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	6585	4	US	AL	HUNTSVILLE
1684520187	302	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	6582	4	US	AL	HUNTSVILLE
1684520188	200	GET	fams.cce.af.mil	/D/1/301843/000/fams.cce.af.mil	JOHN.DOE..xxxxxxxx	pki	a59bb635-45be-4e	3	3	TRUE	TRUE	p	6585	4	US	AL	HUNTSVILLE

Same user with 2 distinct SSO sessions at the same time MAY be valid, but might be an indicator of compromise

If the 2 sessions also come from 2 very different geographies, it is much more likely to be compromised session / credentials

Zero Trust Journey



KEY CROSS-CAPABILITY ELEMENTS

- SASE integration to enable continuous authentication, macro-segmentation security functions
- Continuous logging and inspection of traffic
- Policy enforcement on every transaction

- **Use credentials that comply with NIST 800.64**
- **Context aware authentication**
- **IAL/AAL inform AuthN and AuthZ decistions**

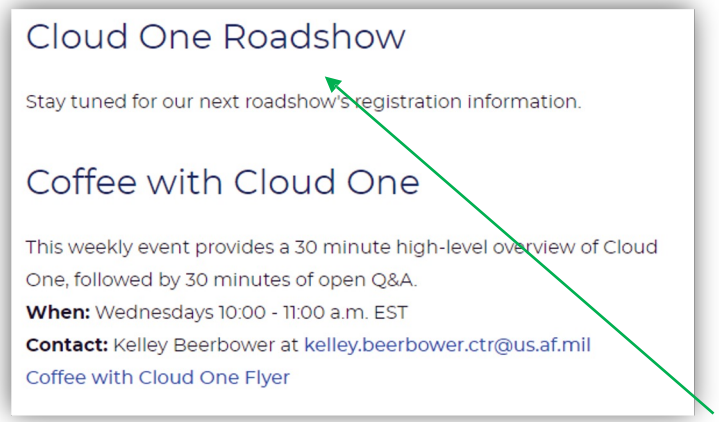
- **Enhance capability**
- **Expand access options**
- **Prioritize user experience**

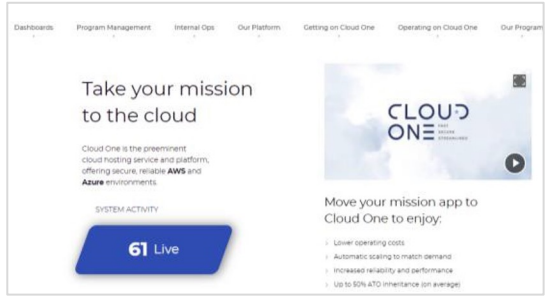
Get Started!

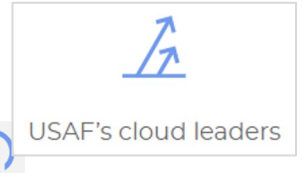
https://info.cloudone.af.mil

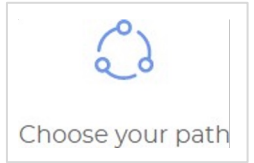
Email: george.calley.1@us.af.mil

Reach out to Service Desk





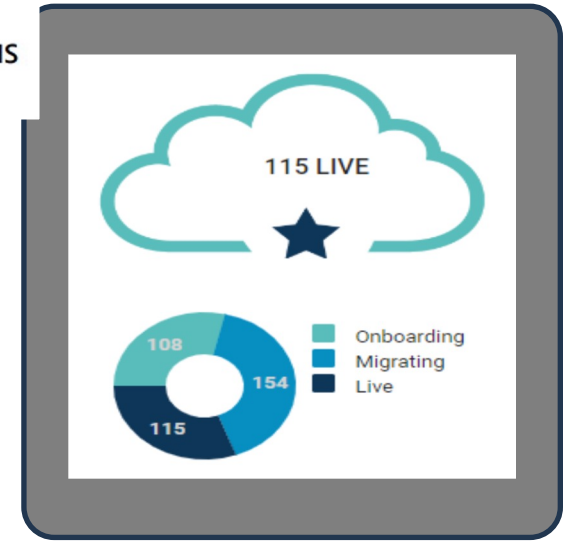




CLOUD ONE FREQUENTLY ASKED QUESTIONS

Keep up with the latest program news and updates

Subscribe to our newsletter or view past newsletters



Thank you

Questions?

Engagement Poll

Let us know how we did! Answer our quick 5 question poll

Coffee with Cloud One

Weekly 30-minute high-level Cloud One overview and a 30-minute Q&A

LinkedIn

Follow Us on LinkedIn for updates and interesting Cloud One stories