



Analog Informatics™
Corporation

AIC Capabilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Analog Informatics Corporation (AIC) builds privileged access, identity, audit, and compliance evidence as modules on one platform: the **AIC Enterprise Privilege Suite™**. AIC Enterprise Privilege Suite™ is the set of modules enterprise buyers score. Modules are sold one by one, so you license only the modules you need and add more later. The suite runs in the cloud or on premises, in a secure enclave, and on air-gapped systems.

AIC Enterprise Privilege Suite™ receives constant feeds, generates alerts, mitigates issues, and constantly checks each system against its baseline configuration where a feed path exists. That makes continuous compliance possible instead of a point-in-time check. Training is free. We work with the reseller, Managed Service Provider, or service provider the customer already uses.

Figure. The AIC Enterprise Privilege Suite™ capability list

Access, identity, audit, evidence, and monitoring sit in one suite instead of separate products.

Alt text: One box labeled AIC Enterprise Privilege Suite™ contains five labeled groups: privileged access, identity, audit, evidence, and monitoring.

Draw: One outer box and five inner labels. Use words and shape. Do not rely on color. Do not show a person.

Screenshot to capture: The main console navigation showing module names, with no host name and no account name. Save it as `images/capabilities-console.png` beside this page when a clean product screen exists. Until that file exists, publish the diagram with this caption and alt text.

How to Read Availability

Availability	Meaning
Available now	The named AIC module ships and works on the systems and paths the suite manages.
Available now, wider scope planned	The module ships. Coverage of systems outside the suite is planned, or stays with the organization.
Planned	The product does not do this yet.
Organization	People, facilities, policy, or tools the organization operates. The Assessment Binder can store the record.

An assessment organization, certification body, or regulator decides whether a requirement is satisfied. These pages describe product availability. They are not an assessment result, a certification, or legal advice.

Capability List

Capability	What It Does	Availability
Privileged Identity Management (PIM)	Discover systems, accounts, privileged group membership, password age, SSH keys, and cloud access keys. Find where each credential is used, change it, and push the new value to every service, task, application pool, COM+ and DCOM application, connection string, and configuration file that uses it. Covers Windows, macOS, Linux and Unix, Active Directory and LDAP, databases, cloud accounts, network and hardware devices, and applications. Extend to any other platform with SSH and Telnet scripts, browser automation, or the REST API (OpenAPI). Vault and check out credentials. See Privileged Identity Management.	Available now
Blast radius	Report how many hosts and services each shared credential reaches, and reduce it by rotating and propagating or by splitting the account into one managed service account per host, with a preview first.	Available now
Browser automation	Change credentials on devices and services that are managed only through a web page. Ready-made automations ship with the suite. Build your own in the console with a visual workflow builder.	Available now

Capability	What It Does	Availability
Privileged Access Management (PAM)	Live SSH, RDP, and VNC sessions in the browser through a broker, approvals, and command restriction that blocks dangerous commands as they are typed.	Available now
Session recording	Recorded SSH, RDP, and VNC sessions with replay.	Available now
Jump	Managed access path for privileged sessions. AIC Enterprise Privilege Suite™ isolates Jump and records sessions.	Available now
Privileged User Management (PUM)	Privilege elevation and delegation management: endpoint elevation, delegation, least privilege, application and command control, just-in-time elevation, and privileged activity auditing. Elevate through the Agent on the system or by remote control from the AIC Server, with one-time activation codes, challenge and response, signed grants, or agentless WinRM and SSH. Windows is the most complete today. Apple Mac and Unix/Linux are expanding. See Privileged User Management.	Available now, wider scope planned
Identity Governance and Administration (IGA)	Account lifecycle and periodic access review for suite accounts. Governance across other applications is planned.	Available now, wider scope planned
Secure Application Launch	Start an application with credentials the user never sees.	Available now
Document sharing vault	Store and share sensitive files with classification marking.	Available now

Capability	What It Does	Availability
Data classification	US government, NATO, and national markings with clearances, mandatory access control, and audited formal release. See Data classification.	Available now
Conditional access	Allow, step up, or deny sign-in by country, network address, multifactor authentication, and session policy. See Conditional access and threat defense.	Available now
Threat intelligence and attack report	Deny sign-in from addresses on threat feeds, and report blocked and failed attempts mapped to MITRE ATT&CK.	Available now
Audit and event forwarding	Privileged-action and session records, Windows Event Log, and syslog in RFC 5424, CEF, or LEEF. Route each event type to its own destinations: Splunk, Microsoft Sentinel, Azure Monitor, Datadog, Amazon CloudWatch, Google Cloud Logging, any web service, another AIC Server, email, and ServiceNow or Jira tickets. Text message notices through seven providers. See Logging, SIEM, and event forwarding.	Available now
Assessment Binder	Living evidence package shared by the assessor, the Managed Service Provider, and the Customer.	Available now
Current State Compliance	Ledger of control findings with rescan.	Available now

Capability	What It Does	Availability
Configuration compliance	Check workstations and servers against STIG-oriented baselines, repair known settings with Fix-It, flag what needs IT, and optionally block a system until it complies. See Configuration compliance.	Available now, wider scope planned
Known default credential detection	Scan networks, match systems and devices to licensed public default-password dictionaries, and flag dangerous defaults still in use. See Known default credentials.	Available now
VM power scheduling	Power off idle workstations and session capacity on a schedule or after idle time, and start them on demand, to cut cloud cost and shrink the attack surface. See VM power scheduling.	Available now, wider scope planned
Incident Response	Incident records, detectors, and email or text alerts when a messaging path is configured.	Available now
Training and attestation	Assign documents to named people and collect a signed attestation.	Available now
Governed mail	Mail for Federal Contract Information or Controlled Unclassified Information inside the suite.	Available now
Cryptography and key custody	AWS-LC, which holds a FIPS 140-3 certificate, on server cryptographic paths. Keys in software, in a PKCS#11 HSM, or in a customer-owned AWS KMS, Azure Key Vault Managed HSM, or Google Cloud KMS key. Separate key sets per system group, with rotation and re-encryption. See Key management.	Available now

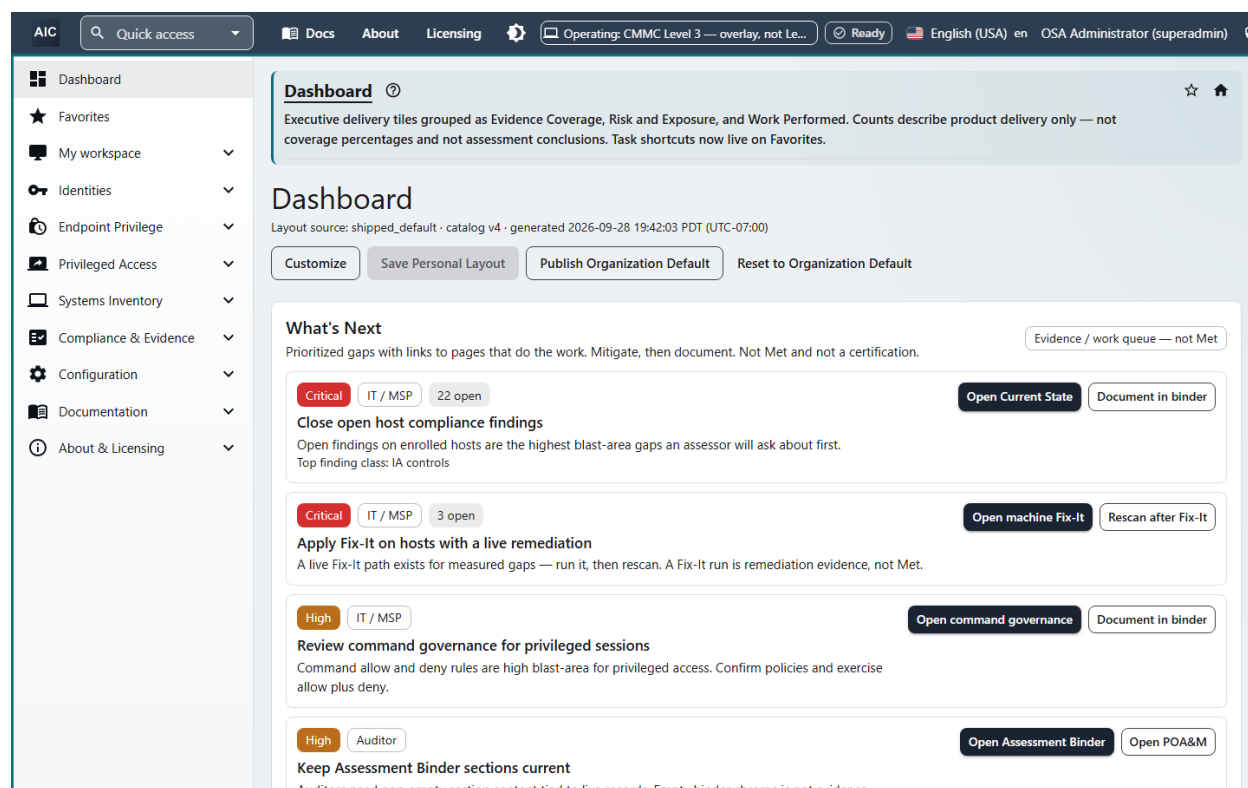
Capability	What It Does	Availability
Directory sign-in	Active Directory and LDAP sign-in, and Microsoft Entra ID, Okta, Ping Identity, and other OpenID Connect and Security Assertion Markup Language (SAML) 2.0 providers, with another step beyond a password.	Available now
High availability	Automatic database failover on customer-supplied hosts.	Available now
Air-gapped operation	AIC Enterprise Privilege Suite™ runs on connected and fully air-gapped systems on Windows, Linux, and Apple Mac, in the cloud or on premises. The Agent rotates passwords on schedule from a shared seed with local propagation and no server connection, and handles elevation on the system itself. See Air-gapped systems.	Available now
Managed Service Provider operation	A Managed Service Provider can administer inside the customer boundary.	Available now
Localization	The operator console ships with 18 language packs. See Localization.	Available now, wider scope planned
Evidence feeds	Records can feed Vanta, Thoropass, and other compliance packages through export and syslog.	Available now
Certificate lifecycle management	Discovery, renewal, and governance of certificates across certificate authorities.	Planned
Cloud infrastructure entitlement management	Analysis of cloud account permissions.	Planned
Vulnerability analysis	Analysis of discovered systems for known vulnerabilities. Planned as an add-on module.	Planned

Capability	What It Does	Availability
Universal host logon banner	One banner pushed to every system.	Planned

The industry terms for these capabilities are on Industry functions.

Screenshots

Screenshots come from a demonstration system. Host names, account names, and network addresses are replaced with sample values.



The dashboard puts the next security and compliance tasks first, with one click to the page that fixes each one.

The screenshot displays the AIC (Analog Informatics Corporation) interface. The top navigation bar includes a search bar, 'Quick access' dropdown, and links for 'Docs', 'About', and 'Licensing'. The main header shows 'Operating: CMMC Level 3 — overlay, not Le...', 'Ready' status, and user information 'English (USA) en OSA Administrator (superadmin)'. The left sidebar contains a menu with items like 'Dashboard', 'Favorites', 'My workspace', 'Identities', 'Endpoint Privilege', 'Privileged Access', 'Overview', 'Vault', 'Sessions', 'Platform overview', 'Connection Points', 'Session Recordings', 'Session Control', 'Jump and capacity', 'Recording operations', 'Policy', 'Access approvals', 'Systems Inventory', 'Compliance & Evidence', 'Configuration', 'Documentation', and 'About & Licensing'. The main content area is titled 'Live-SSH-Session' and describes it as an 'Interactive recorded session viewer'. It shows session details: 'Machine: Linux CUI user workstation', 'OS: Linux version not recorded', and 'Elapsed: 00:18'. Below this, there are controls for 'Back to My Workstations', 'Disconnect', 'Connected', 'Recording: proxy (in progress)', and 'Idle logout 15 minutes'. There are also buttons for 'Enter full screen', 'Font size 100%', 'Launch program', 'Files', and 'Advanced'. A warning message states: '*** COMMAND BLOCKED: `mkfs --version` *** command refused by command-limits (baseline_blocklist): matches baseline dangerous command `mkfs (disk / filesystem destruction)`'. The terminal window shows the following commands and output:
cuiuser@ws-demo-03:~\$ whoami
cuiuser
cuiuser@ws-demo-03:~\$ uname -sr
Linux 6.8.0-136-generic
cuiuser@ws-demo-03:~\$ uptime
08:01:25 up 50 days, 15:26, 4 users, load average: 0.02, 0.01, 0.00
cuiuser@ws-demo-03:~\$ ls -l /etc/os-release
lrwxrwxrwx 1 root root 21 Feb 6 2026 /etc/os-release -> ../usr/lib/os-release
cuiuser@ws-demo-03:~\$ mkfs --version
*** COMMAND BLOCKED: `mkfs --version` ***
command refused by command-limits (baseline_blocklist): matches baseline dangerous command `mkfs (disk / filesystem destruction)`

A live SSH command line, recorded, with a dangerous command blocked as it is typed.

AIC

Quick access

Docs

About

Licensing

Operating: CMMC Level 3 — overlay, not Le...

Ready

English (USA) en

OSA Administrator (superadmin)

Dashboard

Favorites

My workspace

Identities

Endpoint Privilege

Privileged Access

Overview

Vault

Sessions

Platform overview

Connection Points

Session Recordings

Session Control

Jump and capacity

Recording operations

Policy

Access approvals

Systems Inventory

Compliance & Evidence

Configuration

Documentation

About & Licensing

Live-RDP-Session

Interactive recorded session viewer. Disconnect or return to the page you connected to.

Machine: Windows CUI user workstation

OS: Windows version not recorded

Elapsed: 00:27

Back to My Workstations

Log off and disconnect

Disconnect

Connected Recording: proxy (in progress)

Idle logoff 15 minutes

Fit

100%

Scale Fit window

Enter full screen

Ctrl+Alt+Del

Launch program

Files

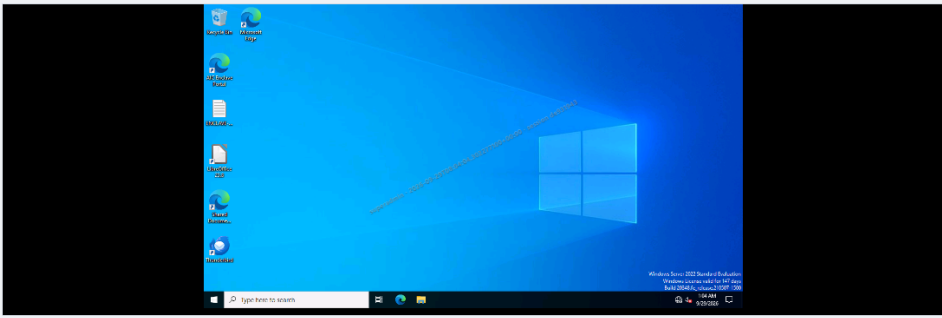
Advanced

FPS

Zoom 49%

Exit full screen Ctrl+Alt+Shift+F

Full screen exit: Ctrl+Alt+Shift+F.



Viewer controls

Copyright 2026 Analog Informatics Corporation.

Administrator personal data is processed for access control and audit. Contact user@example.com.

Admin console data may include CUI. Follow DemoCorp Federal Systems LLC handling rules.

DemoCorp Federal Systems LLC — Information Security Office: CAGE 1DEMO; user@example.com; +1-555-0199 (Mon–Fri 0800–1700 ET)

Compiled program default for DemoCorp Federal Systems LLC. Department: Information Security Office.

A live, recorded RDP desktop session to a Windows workstation, in the browser.

Endpoint Privilege

Sensitive-apps catalog, who may elevate (user, group, or system), default-allow versus approval-required, air-gapped tokens, and host application control.

Control which people, groups, and systems may raise rights on which applications, whether those apps are default-allow or need approval, and how agents work when online or air-gapped.

- Privileged User Management**
Security Technical Implementation Guide (STIG) execution-control packs for Windows, Linux, and macOS. Windows Defender Application Control (WDAC) and AppLocker on Windows; fapolicyd and Gatekeeper pins on other operating systems.
- Applications**
Sensitive-apps catalog with Duration; import bundled or customer CSV.
- Application Groups**
Name a set of apps and bind people, groups, or systems to that set.
- Workstation Prompt**
On-demand elevate helper: pick an app, see allow versus approval, finish online or air-gapped.
- Unix Privilege**
sudo, pbrun, and dzdo as first-class elevation targets.
- Who May Elevate**
Bind IAM users, groups, or systems to apps. Set Default allow or Approval required.
- Elevation Approvals**
Request, approve, or deny time-limited elevation for approval-required apps.
- Elevation Policy**
OS-group offers, duration tiers, and Modes 1-3 channel toggles.
- Air-Gapped Tokens**
Mint or exchange tokens so an agent can elevate while air-gapped.
- Direct Elevation**
Time-bound privileged membership activations on connected endpoints.

Privilege modes you can configure

Endpoint privilege elevation and delegation covers Windows, Unix, approvals, policy, and air-gapped tokens in one place.

Configuration

Unlocated origin

Attack point No events Low High

Origins of blocked and failed access attempts

Country	Code	Blocked	Failed	Unique Addresses
Private network	XA	0	8	1

These numbers describe blocked and failed attempts against this server. They are not proof that attackers ran commands or left malware. Password bars show class and length only. Attempted password values are never stored or shown.

MITRE ATT&CK Coverage

1 technique(s) in 1 tactic(s). Cards appear only when a mapped deny or failure exists.

- CREDENTIAL ACCESS** 8
- Brute Force** 8x

Attack Volume

Each column opens the log that produced it. Empty groups still offer that link. These numbers are delivery counts, not a Met claim.

- TOP SOURCE IPS** 10.20.0.197 8
- MOST-TRIED USERNAMES** admin-x 1

Failed sign-ins are mapped to MITRE ATT&CK technique T1110 Brute Force, with top sources and most-tried usernames.

More on Product screenshots.

Related Pages

- Frameworks
- Capabilities
- Industry functions
- Industry terms AIC supports
- Deployment and integrations
- Continuous compliance
- Air-gapped systems
- Data classification
- Conditional access and threat defense
- Detect, respond, and remediate
- Privileged Identity Management
- Known default credentials
- VM power scheduling
- Configuration compliance
- Localization
- Partners: MSPs, resellers, technology partners and ISVs, service providers, international, and migration
- Glossary
- NIST: SP 800-53
- Industry and privacy: SOC 2, HITRUST, HIPAA, PCI DSS, GDPR, California privacy
- Operational technology: Overview, IEC 62443, NERC CIP
- International: Overview, ISO/IEC 27001, Essential Eight, NIS2
- Product screenshots