The bridge to possible

Cisco Identity Services Engine (ISE)

Aligns to Comply-2-Connect

ISE with C2C is the bridge that helps meet the Defense Department's five-year zero-trust strategy, which outlines a zero-trust architecture that helps secure the entire network. ISE is the ideal Zero Trust (ZT) Policy Decision Point (PDP) which uses adaptive policies to establish trust, enforce trust-based access, continually verify trust, and respond to change in trust. In addition ISE can natively integrate with Cisco networking and security solutions and hundreds of other external solutions which can function as the Policy Enforcement Points (PEP). With ISE, our customers would be able to meet their C2C requirements while concurrently building the foundation of a zero-trust architecture that is effective, easier to manage and help meet their ZT compliance requirements.

The bridge to possible

ISE maps directly into the five steps for C2C compliance and implements commander's intent-based policy for the network.

Step one:

Discover and identify

Establish 100% Visibility

- Detect + identify + categorize
- Asset inventory
  - Hardware
  - Software
  - ICS/SCADA/OT

ISE is uniquely positioned to harness the untapped telemetry in your network to provide end-to-end visibility without the use of span ports or TAPs. IT administrators can automatically detect, identify, and categorize all endpoints connecting to the network, no matter where they are connecting from With a simplified approach to network access control, asset inventories for hardware and software are automated and all data is visualized and exportable to upstream dashboards to ease reporting and enable step 2.

Step two:

Interrogate

Compliance Posture

- Scan device properties
- Determine compliance state
- Report scan
- Alert remediation tools

To establish trust and reduce risk, ISE employs multiple standards-based authentication methods, including 802.1x, a DISA CAT 1 STIG, and MAB (MAC Authentication Bypass), to meet C2C requirements. ISE supports both agentless and agent-based posture to verify that the endpoint or device meets DoDIN-defined security policies before authorizing access and to satisfy step 2 requirements.

Step three:

Auto-remediate

Perform Compliance Remediation

- Automate remediation actions
- Validate and report findings
- Monitor changes and updates

Auto-remediation with ISE is a seamless experience that has little impact on the network or user experience and relieves strained IT personnel. Network operations can bring devices into compliance within a specified time window or restrict network access all together based on the organization's risk tolerance for any one profiled group of endpoints. Pre- and post-authentication checks ensure that the organization's risk levels are always maintained to meet step 3 of C2C and enable step 4.

Step four:

Authorize connection

Establish Access Level of Device

- Quarantine non-compliant
- Assign compliant device to proper segment

ISE provides contextual visibility and control across all connection mediums. This enables administrators to not just authorize access but control it by segmenting access based on device/user profile and categorization obtained in step 1. ISE sets policy to ensure users and devices only gain access to the network resources required to meet mission objectives. This level of granular control sets the building blocks for a zero-trust architecture that strengthens any defense-in-depth strategies. If an endpoint falls out of compliance, ISE quarantines the device to perform auto-remediation as outlined in step 3.

Step five:

Situational awareness and enforcement

Enforce Policy

- Monitor for config change
- Re-authenticate and control devices
- Orchestration with other capabilities

With a level of deep contextual visibility that enables proper identification and classification, ISE can continually verify that all endpoints connecting to the managed infrastructure are in, and remain in, compliance throughout the entire session. ISE takes context from across your entire security stack to enable continuous trusted access, providing protection beyond authorization and extending C2C. Open APIs simplify reporting in any console to enable rapid remediation and ensure the least amount of impact to both IT and mission-critical objectives.

The bridge to possible

Key benefits of comply-to connect

- See, know, identify, and classify all “things” connecting to the managed infrastructure
- Ensure compliance before authorizing access to network resources
- Continuous evaluation with automated response to maintain compliance

Why ISE

ISE is the industry’s most widely adopted and awarded network access and control solution. ISE has maintained market dominance with a platform approach to securing access that is integrated, not bolted into the network.

With ISE, DoD teams are closing the gaps for device visibility—enabling the DoD’s network management and security strategies.

Cost

- $1.6M saved byavoiding security events over three years
- TCTO proven to be 50% less than competition

Simplicity

- Security simplified with BYOD and guest access built in
- Unrivaled scalability Secure 2M+ endpoints in a cluster

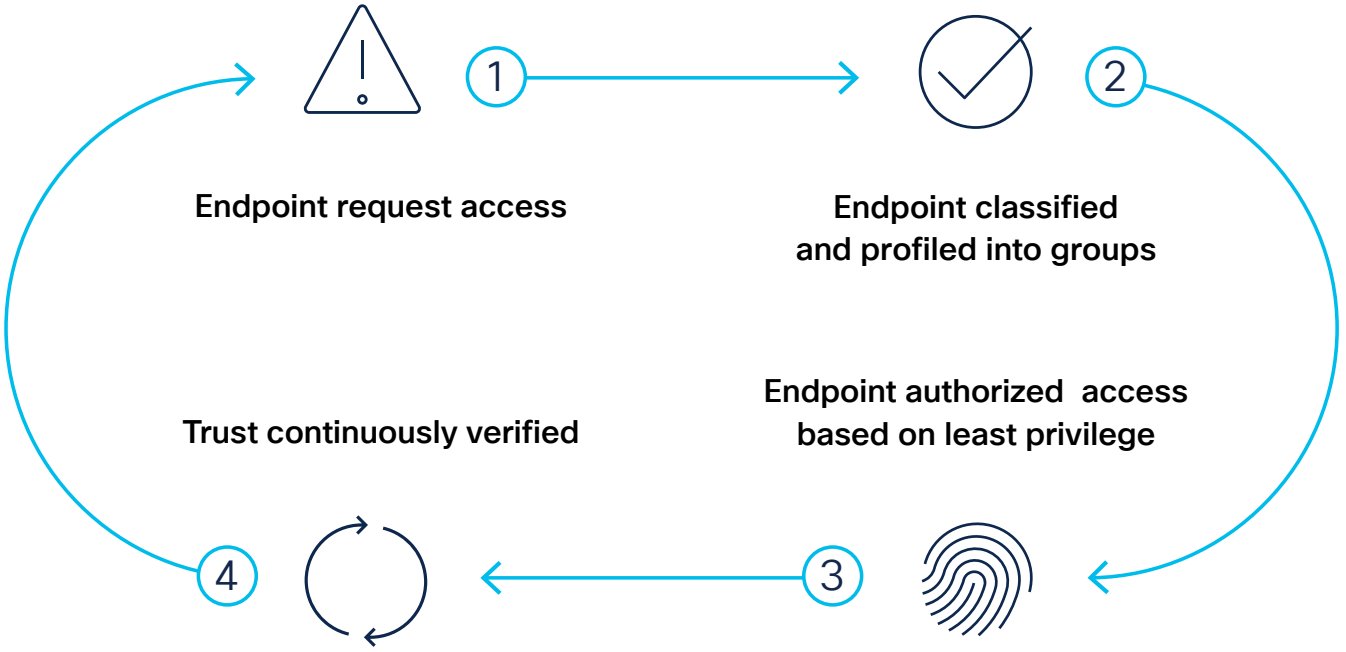
Ongoing ROI

- Foundation for zero trust and continual trusted access
- Increase ROI with TACACS+ /Device Admin without additional hardware

Proven

- APL certified
- DISA PMO Approved
- 3 million+ DoD endpoints covered by ISE

The bridge to possible



1. Endpoint request access

- Endpoint is identified and trust is established
- Posture of endpoint verified to meet compliance

2. Endpoint classified and profiled into groups

- Endpoints are tagged w/ SGTs
- Policy applied to profiled groups based on least privilege

3. Endpoint authorized access based on least privilege

- Access granted
- Network segmentation achieved

4. Trust continuously verified

- Continuously monitors and verifies endpoint trust level
- Vulnerability assessments to identify indicators of compromise
- Automatically updates access policy

C45-4238057-00 03/24