Simplifying Comply-to-Connect for DoD Stakeholders

Empower Secure Operations with Comply-to-Connect (C2C)

Overview

The United States Department of Defense (DoD) has set a high bar for its components and stakeholders to securely access DoD information and systems, with evolving policy mandates that broadly impact government and business partnerships. Comply-to-Connect (C2C) is the automated approach the DoD uses to control what devices are allowed to authenticate and connect to the DoD Information Network (DoDIN). C2C requires that devices are automatically fixed if they are found out of compliance, and that specific reporting and visibility into the whole process is provided. DoD's evolving, complex, and multi-phased mandate requires an essential set of integrated capabilities to secure these mission-critical environments.

C2C capabilities also form a foundational stepping stone to Zero Trust–another much broader phased security mandate the DoD is navigating. There are similar security requirements across U.S. Federal civilian and intelligence agencies.

Simplifying C2C

The Cisco® approach simplifies C2C for the DoD and supporting organizations through an integrated, flexible, and efficient bundle to meet these milestones and achieve Full Operating Capability (FOC) across the Secret Internet Protocol Router Network (SIPRNet) and Non-classified Internet Protocol Router Network (NIPRNet).

The Cisco C2C bundle combines the best-in-class Cisco Identity Services Engine (ISE); Splunk's industry-leading platform, Security Information and Event Management (SIEM), and Security Orchestration, Automation, and Response (SOAR); and Cisco Customer Experience (CX) integration and deployment services. The C2C Reporting Application supports up to C2C Step 3 with a fixed-format ISE-based reporting application, essential C2C integrations, and limited orchestration capability. The C2C Reporting Application Advantage supports all C2C steps (FOC) by adding comprehensive and customizable C2C reporting dashboards, advanced C2C integrations, and advanced orchestration capability. The C2C bundle also flexibly supports DoD organizations with existing ISE or Splunk deployments.

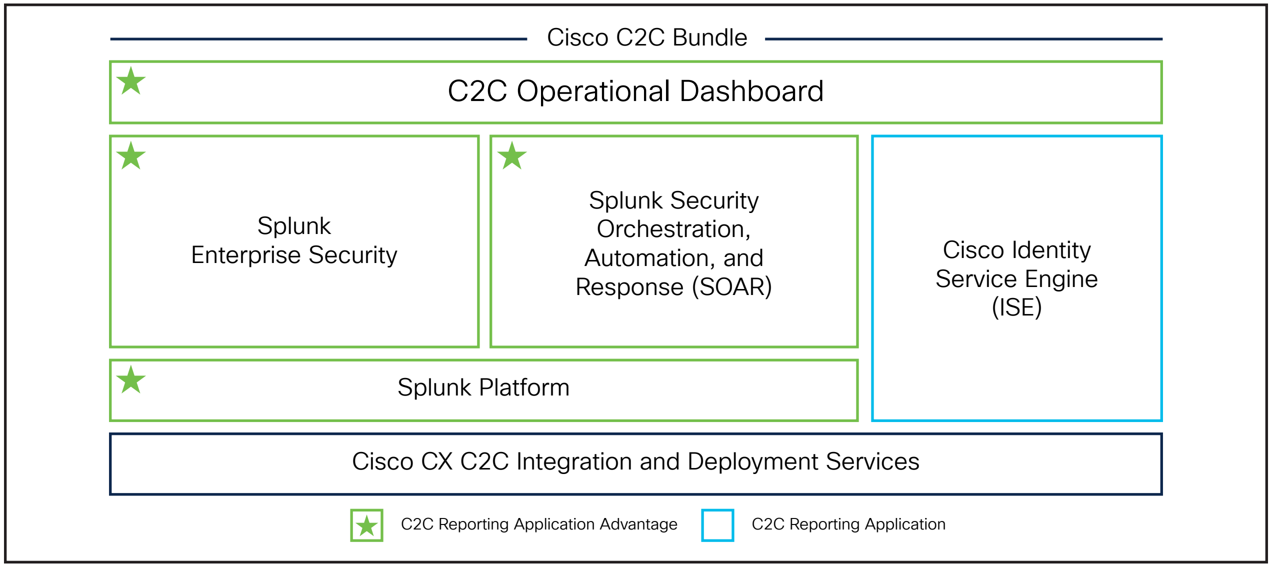

Cisco C2C Bundle
★ C2C Operational Dashboard
★ Splunk Enterprise Security
★ Splunk Security Orchestration, Automation, and Response (SOAR)
Cisco Identity Service Engine (ISE)
★ Splunk Platform
Cisco CX C2C Integration and Deployment Services
★ C2C Reporting Application Advantage
□ C2C Reporting Application

Figure 1. The Cisco C2C bundle

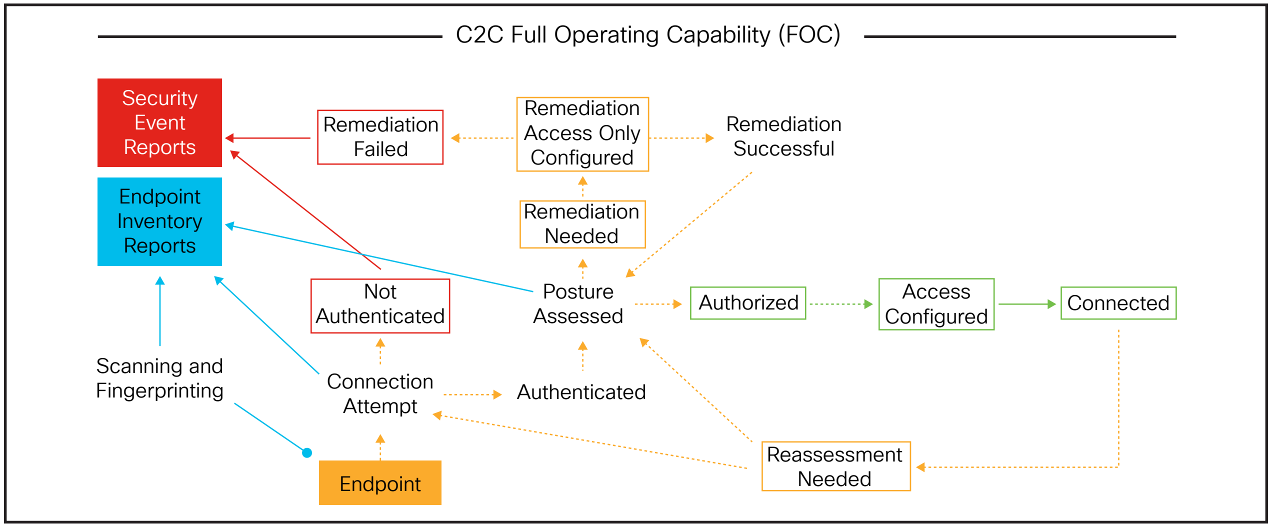
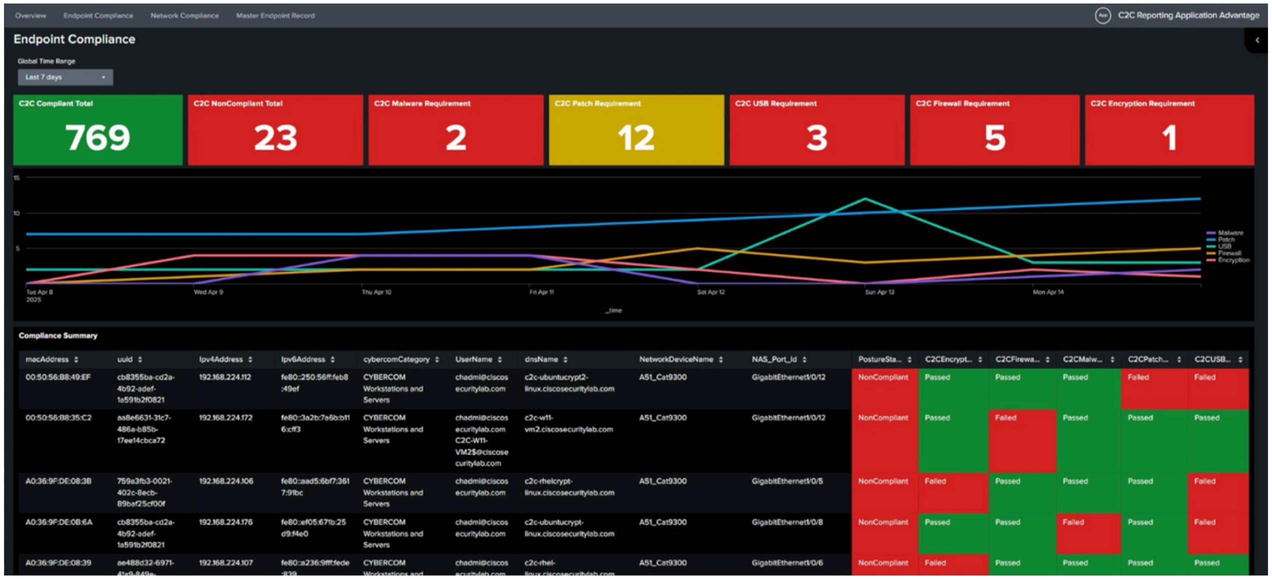


Figure 2. The Cisco C2C bundle accelerates Full Operating Capability (FOC)

Solution capabilities

The Cisco Comply-to Connect bundle provides your organization with a comprehensive set of capabilities:

- Proactively identify and inventory all C2C endpoint categories: mobile phones, laptops, servers, printers, network infrastructure, IoT devices, weapons systems, and everything in between; with visibility wherever the endpoint is: wired, wireless, in the cloud, or even temporarily offline.
- Authenticate endpoints against a wide variety of Identity, Credential, and Access Management (ICAM) systems and policies, and leverage multiple endpoint attributes to authenticate more complex endpoints including IoT devices and mission-control systems.
- Take a massive amount of insight and context from mobile and endpoint device management systems, Assured Compliance Assessment Solution (ACAS), Host-Based Security System/Enterprise Security System (HBSS/ESS), and many others to make the most informed posture assessment.
- If an endpoint is found out of compliance, the system will isolate it and attempt to remediate the issue automatically.
- Automatically open a trouble ticket with Information Technology Service Management (ITSM) if the system determines manual intervention is required.
- Since networks are dynamic environments, and the threat landscape is constantly shifting, any indication of breach or compromise can trigger an automatic reassessment of the endpoint, potentially limiting the impact of a security incident.
- Support a variety of network access device vendors, leveraging existing investments.
- Consolidate every piece of endpoint profile data drawn from each integrated platform into a comprehensive, C2C-compliant endpoint inventory report and security posture visibility dashboard, also allowing for Governance, Risk Management, and Compliance Management (GRC) integration when your organization is ready.



Endpoint Compliance

Global Time Range: Last 7 days

C2C Compliant Total	C2C NonCompliant Total	C2C Malware Requirement	C2C Patch Requirement	C2C USB Requirement	C2C Firewall Requirement	C2C Encryption Requirement
769	23	2	12	3	5	1

Compliance Summary

macAddress	uuid	Ipv4Address	Ipv6Address	cybercomCategory	UserName	dnsName	NetworkDeviceName	NAS_Port_Id	PostureSta...	C2CEncrypt...	C2CFirewa...	C2CMalw...	C2CPatch...	C2CUSB...
00:50:56:B8:49:EF	cb8355ba-cd2a-4b92-adef-1a591b2f0821	192.168.224.112	fe80::250:56ff:feb8:49ef	CYBERCOM Workstations and Servers	chadmi@ciscosecuritylab.com	c2c-ubuntucrypt2-linux.ciscosecuritylab.com	A51_Cat9300	GigabitEthernet1/0/12	NonCompliant	Passed	Passed	Passed	Failed	Failed
00:50:56:B8:35:C2	aa8e6631-31c7-486a-b85b-17ee14cbca72	192.168.224.172	fe80::3a2b:7a6b:b116:cff3	CYBERCOM Workstations and Servers	chadmi@ciscosecuritylab.com C2C-W11-VM2$@ciscosecuritylab.com	c2c-w11-vm2.ciscosecuritylab.com	A51_Cat9300	GigabitEthernet1/0/12	NonCompliant	Passed	Failed	Passed	Passed	Passed
A0:36:9F:DE:08:3B	759a3fb3-0021-402c-8ecb-89baf25cf00f	192.168.224.106	fe80::aad5:6bf7:3617:91bc	CYBERCOM Workstations and Servers	chadmi@ciscosecuritylab.com	c2c-rhelcrypt-linux.ciscosecuritylab.com	A51_Cat9300	GigabitEthernet1/0/5	NonCompliant	Failed	Passed	Passed	Passed	Failed
A0:36:9F:DE:0B:6A	cb8355ba-cd2a-4b92-adef-1a591b2f0821	192.168.224.176	fe80::ef05:671b:25d9:f4e0	CYBERCOM Workstations and Servers	chadmi@ciscosecuritylab.com	c2c-ubuntucrypt-linux.ciscosecuritylab.com	A51_Cat9300	GigabitEthernet1/0/8	NonCompliant	Passed	Passed	Failed	Passed	Failed
A0:36:9F:DE:08:39	ae488d32-6971-41a9-849e-	192.168.224.107	fe80::a236:9fff:fede:839	CYBERCOM Workstations and	chadmi@ciscosecuritylab.com	c2c-rhel-linux.ciscosecuritylab.com	A51_Cat9300	GigabitEthernet1/0/6	NonCompliant	Failed	Passed	Passed	Passed	Passed

Figure 3. One of the C2C Application Reporting Advantage dashboards in the Cisco C2C bundle

Use cases

The DoD C2C mandate describes specific milestones and use cases that all DoD components must achieve to be considered compliant. The current target is FOC by June 2026.

DoD C2C Mandate

Step 1 - January 2022	Step 2 - September 2023	Step 3 - September 2024	Step 4 - September 2025	Step 5 - June 2026
Discovery, Identification, and Categorization	**Interrogation**	**Automatic Remediation**	**Authorize Connection**	**Policy Enforcement and Situational Awareness**
• Establish policy to rapidly identify and categorize devices that are reported as unknown/unauthorized • Assign devices to established endpoint categories • Deploy Security Policy orchestrator • Identify and block shadow IT/unauthorized endpoints • Determine what actions will be automated/manual* • Implement initial Network Access Control (NAC) • Establish near-real time awareness of all devices • Determine level of automation workflow* • Establish and inventory of all authenticated and authorized devices, publish HW/SW inventory to designated repository	• Ability to segregate devices prior to full network connection • Verify security compliance • Periodically revalidate configuration of endpoints currently connected to the environment	• Separate non-compliant endpoint to a remediation VLAN or implement appropriate Access Control List (ACL) to restrict access to necessary remediation processes only • Automatically determine remediation steps required • Automatically implement remediation steps • Automatically validate STIG compliance • Monitor changes since last contact with device • Validate remediation actions • Generate a report of actions taken, generate a trouble ticket if automation fails	• Full NAC capability will deny, or provide limited or full device access based on device security configuration, vulnerability management compliance, device type, and location • Validate devices seeking access to various network segments • Establish and automate access level of device • Quarantine non-compliant devices • Integrate with ICAM • Complete operational performance assessment*	• Non-compliant machines or users will not be given DODIN access • Guest networks established • Continuously assess device configuration compliance • Threats or vulnerabilities identified will leverage automated or manual mitigation processes • C2C will block network access to non-compliant endpoints and attempt to remediate • Fully integrate with the selected ICAM and GRC solutions

All technical elements of the 5 steps are functions of the Cisco C2C solution except * **Procedural** (3) items

“Cisco’s approach simplifies C2C for your organization to meet this complex, multi-phased security mandate.”

“Cisco’s integrated, flexible, and efficient C2C bundle helps your organization achieve Full Operating Capability (FOC) across SIPRNet NIPRNet.”

Leverage Cisco CX and trainings for C2C guidance

A critical part of how Cisco simplifies C2C is through our CX organization. These professional services resources are experts in C2C and its associated technologies and have worked across the DoD supporting C2C deployments and integrations. Cisco has also created comprehensive C2C training to ensure that you are prepared to operate these environments. Cisco CX and our trusted partners have some compelling C2C Day Two support options as well if your organization wants additional guidance and expertise.

Cisco Capital

Financing to help you achieve your objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

The Cisco Advantage

Cisco offers the most efficient and comprehensive solution to help DoD stakeholders navigate the complexities of the C2C mandate. Our cost-effective, integrated bundle simplifies C2C requirements while leveraging your existing investments, making it a natural extension of your current setup. With customizable, end-to-end reporting and dashboards, you’ll gain clear visibility into your C2C progress. Whether starting from scratch or enhancing existing solutions, Cisco ensures you achieve FOC compliance as seamlessly and efficiently as possible.

Secure your mission-critical operations today.

Contact your Cisco account team to learn more about how Cisco’s C2C bundle can help simplify your C2C and Zero Trust journey. Additionally, visit cisco.com/go/c2c to explore C2C training options, available both on-demand and live.