U.S. Air Force Comply to Connect: Understand the Requirements

The Need for Comply-to-Connect Solutions

Evolving continually, the Air Force Network, known as AFNet, is the critical fabric that connects airmen to mission-critical information, applications, and services. Today, AFNet is undergoing unprecedented change. One reason is the Joint Information Environment (JIE), established to increase IT efficiencies, lower costs, and improve information sharing. JIE increases the importance of situational awareness. Network operators need to know who is connected to AFNet at any time, what devices are being used, and the security status of those devices. They also need better control over the traffic flowing across the network. And all of this needs to happen with less manpower.

This challenge is complicated in the Internet of Things (IoT) era as AFNet connects more types of devices. In addition to wired workstations, servers, and printers, it connects wireless devices, video surveillance IP cameras, physical access controls, and building environmental sensors. Personnel now connect using many more types of devices than they did before and from more locations.

New ways of working require a more nuanced approach to security. In particular, it has become essential to interrogate both the user and the device before granting access to the network.

Comply-to-Connect solutions fulfill this need. These solutions take a standards-based approach to security. The goal is to always know what devices are on your network and to control what resources they can access. This helps to mitigate existing risks such as:

- Propagation of malware that can lead to data exfiltration, network outages, or denial of service
- Unauthorized people accessing information by using authorized devices
- Authorized personnel using unauthorized devices such as personal laptops or tablets

This white paper lists five main areas concerning your network, and our recommended capabilities that a comprehensive Comply-to-Connect solution should feature.

What You Will Learn

This white paper is intended for U.S. Air Force leaders and requirement writers. It explains capabilities required of a successful Comply-to-Connect solution, such as:

- Verifying identity of users and devices
- Preventing propagation of malware that can lead to network infiltration or data exfiltration
- Controlling user access to resources based on authorization
- Knowing who and what is connected to the network at any time, and what they are doing
- Minimizing manpower to operate and maintain networks
- Complying with Department of Defense (DoD) and U.S. Air Force policies for information assurance

1. Verify Identity of Users and Devices

The Air Force needs to know the identity of every person attempting to access the network. This includes active duty personnel, contractors, military dependents, and visitors and guests. The Air Force currently authenticates DoD users using their Common Access Card (CAC) credentials.

However, granting network access to the user before also authenticating the device is risky. The device might be infected. It might not be government owned. Even if the device is permitted, it might not have the latest operating system patches, exposing the network to risk from malware, virus propagation, and denial-of-service attacks. Another risk of granting access before authenticating the device is that someone who connects with a non-Microsoft Windows device could potentially access data and applications without detection.

The Air Force currently uses port-based security to control which devices can connect. This involves checking the device's MAC address against a list of MAC addresses that are allowed to access that particular network port. The list is manually created and maintained.

Port security has three shortcomings. First, it does not work with wireless devices, including laptops and tablets. Second, when a computer is moved from one location on base to another, a network administrator needs to program the new network port to allow the computer to connect. This process is time consuming, manpower intensive, and error prone. Third, spoofing MAC addresses is an easy way to circumvent existing security procedures.

Some bases have started using Cisco® Secure Access Control Server (ACS) and MAC authentication bypass (MAB). MAB addresses one shortcoming of port security by making it easier to tie the device's MAC address to the network port it is allowed to access. However, MAB does not fully satisfy Comply-to-Connect requirements. It does not validate the device's security posture or protect against MAC spoofing. Lastly, it does not control access to resources based on the user identity, device type, or device location. Management overhead is high because the network administrator needs to maintain a list of valid MAC addresses that are authorized to access the network.

Comply-to-Connect solutions should include the following capabilities:

- Ability to create device profiles, including:
  - » Device ownership: Only permitted devices are allowed to access the network.
  - » Device type: A tablet needs different privileges than a printer or IP phone, for example.
  - » Manufacturer: This is useful for inventory reports.
  - » Operating system: The Air Force currently allows connections from desktops and laptops operating Microsoft Windows software. Connections from IP phones, smartphones, and tablets are beginning to be permitted.
- Central management of all devices to minimize staff overhead: Look for a management solution that works with the IEEE 802.1X protocol and MAB, and functions whether or not you are using Active Directory.
- Dynamic device profiling to create and maintain a MAB database: This reduces manpower requirements and avoids human error.

2. Prevent Propagation of Malware

Malware can lead to network infiltration or data exfiltration. To mitigate the threat, the network should assess the device's security posture before allowing it to connect and automatically remediate out-of-compliance devices. The network needs to be smart enough to treat different devices differently. For example, a version of an operating system might be denied in most cases but permitted on a highly controlled system such as a critical medical device or aircraft support system.

Comply-to-Connect solutions should include the following capabilities:

- Ability to determine whether a device complies with security posture: The security profile should include, at minimum, the latest operating system patches and antivirus software.
- Automatic remediation: The device authentication solution should quarantine devices that are out of compliance and quickly remediate them without effort from the user. Automatic remediation saves time for the IT support team. It also improves productivity because personnel do not have to wait for help desk support.
- Ability to create custom profiles for unique government devices: Examples include proprietary computer systems and devices such as aircraft maintenance systems.

3. Control User Access to Resources Based on Authorization

Not all authorized users should have access to all resources. For example, only certain individuals should have access to information about active personnel or payroll data. Vendors and guests should be able to connect only to the Internet.

To authorize users to access specific network resources, the Air Force currently matches CAC credentials to Active Directory. This approach works well for resources controlled by Microsoft Windows servers. However, it does not work for other resources connected to the network. Examples include workstations that use another operating system, scanners, and printers. Relying exclusively on Active Directory introduces the risk of data exfiltration, man-in-the-middle attacks, and denial-of-service attacks. The answer is to use both the network and Active Directory to authenticate users and devices.

Comply-to-Connect solutions should include the following capabilities:

- VLAN and Virtual Routing and Forwarding (VRF) support: After authorizing the user and authenticating the device, the network should connect the device to the appropriate VLAN or VRF. The guest VLAN provides Internet access only. Other VLANs provide access to all or a subset of Air Force resources.
- Access control lists (ACLs) for wired and wireless connections: After a user is authenticated, access is granted based on the user's identity and permissions.
- Security group tags: Using tags, administrators can centrally create and manage access control policies for user groups and resources. Network devices inspect the tags as traffic enters the network. At each hop, they decide whether to allow or drop traffic. Tags enable consistent policy enforcement. They also allow administrators to see everything that is connected to the network.

4. Know Who and What Is Connected to the Network at Any Time

Knowing the context of every connection request is important for several reasons. Context is required for Command Cyber Readiness Inspections (CCRI) and other security audits. Knowing device context also provides situational awareness for network operators. Reports that include detailed asset information show which components are nearing end of life. Reports can also aid in investigations by showing the identity of the user and the type of device generating traffic on a given network port.

Comply-to-Connect solutions should include the following capabilities:

- Visibility: Administrators need reports that provide contextual information about each user and endpoint that attempts to connect to the network. Information should include user identity, device, manufacturer, user location, time of day, and type of network connection (wired, wireless, or VPN).
- Flexible sorting options: It is useful to be able to sort devices by manufacturer, operating system version, antivirus software version, and windows patch level.
- Integration with security information and event management (SIEM) systems: Integration with SIEMs, such as HP ArcSight and Splunk, increases visibility.

5. Minimize Manpower to Maintain and Operate Networks

TCO for security solutions includes three factors: capital expense, operational expense, and discovery and remediation costs after a security incident occurs. Automated processes can greatly reduce the manpower needed to maintain the network. For example, device authentication and profiling eliminate the need to manually create and maintain the list of authorized MAC addresses for MAB.

Comply-to-Connect solutions should include the following capabilities:

- Automated network admission control and port security: One DoD customer was able to increase the percentage of incidents resolved according to the service-level agreement (SLA) from 70 percent to 95 percent. Another customer reported that help desk wait time decreased by an average of 75 percent.
- Automated application of security patches when a device connects: This saves time for the IT team as well as the user. A civilian research agency reduced IT help desk cases by 60–70 percent by using Cisco Identity Services Engine (ISE) for device authentication.
- Device consolidation: Fewer devices mean less space and lower power, cooling, and management costs. Look for solutions that combine user and device authentication, guest access support, mobile device management (MDM), and bring-your-own-device (BYOD) integration.
- Features that simplify deployment and operation: Automation lowers costs and reduces errors.

Why Cisco?

The United States DoD has been using Cisco solutions for more than two decades. The Air Force currently takes advantage of Cisco technology for its networks, data center, and voice and video collaboration.

The Cisco Comply-to-Connect solution is a combination of products to identify, protect, and secure devices (Table 1). The solution works with devices in any location, whether they connect over wired, wireless, or VPN connections. It decides whether to admit a device before granting it access to the network.

Based on industry-standard protocols, such as IEEE 802.1X, the Cisco Comply-to-Connect solution provides protection before, during, and after attacks:

- **Before an attack:** You can't protect what you can't see. Knowing what is on your network helps you set up access controls, enforce security policies, and block applications and access to critical assets.
- **During an attack:** When attacks do occur, detect and block them everywhere the threat appears. This includes networks, endpoints, mobile devices, and virtual environments.
- **After an attack:** Quickly determine the scope of the damage, remediate, and bring operations back to normal as quickly as possible.

Table 1

Comply-to-Connect Requirement	Cisco Comply-to-Connect Solution
Verify identity of users and devices	• Identifies devices on the network and matches them against device access policies
Prevent propagation of malware	• Automatically remediates authorized devices that have fallen out of compliance with security policy. Remediation often takes just a few minutes • Automatically pushes updates for any device such as laptops and tablets • Enforces custom profiles that can be created for specialized computer systems
Control user access to resources based on authorization	• Provides visibility into who and what is connected to the network • Allows complete control over all network entry points: wired, wireless, and VPN
Know who and what is connected to the network at any time, and what they are doing	• Dynamically detects and classifies every endpoint connected to the network • Matches the devices to a device profile: operating system, mobile client, and non-user endpoints such as printers and video surveillance cameras
Minimize manpower to maintain and operate networks	Cisco automation tools: • Cisco IOS® device sensor, built in to Cisco access switches: Creates device profiles for laptops, wireless access points, video surveillance cameras, and more • Cisco Flexible Authentication: Configures the sequence and priority of IEEE 802.1X, MAB, and switch-based web authentication • SNMP Probe: Gathers information about end devices • IEEE 802.1X extensions, including MAB and downloadable ACLs (DACLs): Applies an ACL when the device is authorized

The Cisco Comply-to-Connect solution helps the Air Force comply with all the following requirements:

- Compliance with Security Technical Implementation Guides (STIGs).
- Compliance with DoD Instruction 8420.01, "Commercial WLAN Devices, Systems, and Technologies."
- Compliance with Defense Information Systems Agency (DISA) Unified Capabilities Requirements (UCR).
- Compliance with U.S. Air Force Base Area Network functional specification.
- Supports 802.1X protocol with the extensible authentication protocol (EAP).
- Compliance with Federal Information Processing Standards (FIPS) and Common Criteria encryption standards.
- Support for RADIUS Change of Authorization (CoA). This feature makes it possible to change the attributes of an authentication, authorization, and accounting (AAA) session after authenticating the user. Cisco ISE supports CoA. When a policy changes for a user or user group, administrators can send the RADIUS CoA packets from Cisco ISE to reinitialize authentication and apply the new policy.

Products in the Cisco Comply-to-Connect Solution

- Cisco routers, switches, and firewalls
- Cisco ISE
- Cisco Secure ACS
- Cisco Cyber Threat Defense Solution
- Cisco wireless controllers

For More Information

To read a paper about policy-governed networks, visit: www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/white_paper_c11-663616.pdf.

To learn more about Cisco Unified Access™ solutions, visit: www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

To learn about the latest Internet security threats, read the Cisco 2014 Annual Security Report: https://info.sourcefire.com/2014CiscoAnnualSecurityReport-Social.html.