



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTE)

28 October 2020

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Extension of the Joint Interoperability Certification of the Aruba ClearPass Policy Manager with Software Release 6.9.2

- References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013, Change 1," June 2015
(c) through (e), see Enclosure

1. Certification Authority. Reference (a) establishes the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for Department of Defense Information Network (DODIN) products, Reference (b).

2. Conditions of Certification. The Aruba ClearPass Policy Manager with Software Release 6.9.2, hereinafter referred to as the System Under Test (SUT), meets all critical interoperability requirements of the Unified Capabilities Requirements (UCR), Reference (b), and is certified for joint use as a Network Access Control (NAC) with the conditions described in Table 1. This certification expires upon changes that affect interoperability, but no later than the expiration date specified in the DODIN Approved Products List (APL) memorandum.

This extension of the certification is for Desktop Review (DTR) 5. DTR 5 was requested to update the SUT Software Release version from 6.7.3 to 6.9.2. See Paragraph 4 for additional details.

Table 1. Conditions

Table with 3 columns: Condition, Operational Impact, Remarks. Rows include Open Discrepancies, UCR Waivers, and None.

Enclosure

Table 1. Conditions (continued)

Condition		Operational Impact	Remarks												
TDR#	Conditions of Fielding (CoF)														
001	IP6-000540 - The product shall support the capability to disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.	Minor with POA&M	CLOSED (See note.)												
001	IP6-000550 - If the product has the capability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address, the product shall support the disabling of this capability.	Minor with POA&M	CLOSED (See note.)												
TDR#	Open Test Discrepancies														
	None (See note.)														
<p>NOTE(S): The DISA adjudication board accepted a POA&M date of 15 July 17 and added a CoF that the device must be positioned behind a firewall on both its internal and external interfaces. The vendor updated their LoC with DTR 2, showing compliance for IP6-000540 and IP6-000540; therefore, the corresponding test discrepancies were CLOSED.</p> <p>LEGEND:</p> <table> <tr> <td>APL</td> <td>Approved Products List</td> <td>IPv6</td> <td>Internet Protocol version 6</td> </tr> <tr> <td>CoF</td> <td>Conditions of Fielding</td> <td>POA&M</td> <td>Plan of Action and Milestones</td> </tr> <tr> <td>DISA</td> <td>Defense Information Systems Agency</td> <td>SUT</td> <td>System Under Test</td> </tr> </table>				APL	Approved Products List	IPv6	Internet Protocol version 6	CoF	Conditions of Fielding	POA&M	Plan of Action and Milestones	DISA	Defense Information Systems Agency	SUT	System Under Test
APL	Approved Products List	IPv6	Internet Protocol version 6												
CoF	Conditions of Fielding	POA&M	Plan of Action and Milestones												
DISA	Defense Information Systems Agency	SUT	System Under Test												

3. Interoperability Status. Table 2 provides the SUT interface interoperability status, Table 3 provides the Capability Requirements and Functional Requirements status and Table 4 provides a DODIN APL product summary.

Table 2. Interface Status

Interface (See note.)	Applicability (R), (O), (C)			Status	Remarks																				
Product Interfaces																									
10BASE-X	R	R	R	Met	None																				
100BASE-X	R	R	R	Met	None																				
1000BASE-X	R	R	R	Met	None																				
10GBASE-X	R	R	R	Not Applicable	None																				
40GBASE-X	R	R	R	Not Applicable	None																				
100GBASE-X	R	R	R	Not Applicable	None																				
Network Management Interfaces (See note.)																									
10BASE-X	R	R	R	Met	None																				
100BASE-X	R	R	R	Met	None																				
1000BASE-X	R	R	R	Met	None																				
<p>NOTE(S): The UCR 2013 Change 1, Section 13 does not identify individual interface requirements for security devices. The SUT must minimally provide Ethernet interfaces that meet the requirements in Section 2.7.1.</p> <p>LEGEND:</p> <table> <tr> <td>Base-X</td> <td>Megabit Baseband Ethernet over Fiber or Copper</td> <td>Mbps</td> <td>Megabits per second</td> </tr> <tr> <td>C</td> <td>Conditional</td> <td>O</td> <td>Optional</td> </tr> <tr> <td>CR</td> <td>Capability Requirements</td> <td>R</td> <td>Required</td> </tr> <tr> <td>FR</td> <td>Functional Requirements</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>GBASE-X</td> <td>Gigabit Ethernet over Fiber or Copper</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> </table>						Base-X	Megabit Baseband Ethernet over Fiber or Copper	Mbps	Megabits per second	C	Conditional	O	Optional	CR	Capability Requirements	R	Required	FR	Functional Requirements	SUT	System Under Test	GBASE-X	Gigabit Ethernet over Fiber or Copper	UCR	Unified Capabilities Requirements
Base-X	Megabit Baseband Ethernet over Fiber or Copper	Mbps	Megabits per second																						
C	Conditional	O	Optional																						
CR	Capability Requirements	R	Required																						
FR	Functional Requirements	SUT	System Under Test																						
GBASE-X	Gigabit Ethernet over Fiber or Copper	UCR	Unified Capabilities Requirements																						

Table 3. Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (High-Level) (See notes 1 and 2.)	UCR 2013 Change 1 Reference	Status
1	Cybersecurity (R)	4	Met
2	IPv6 (R)	5	Met
3	Security Device Requirements (R)	13.2	Met

NOTE(S):
 1. The annotation of 'required' refers to a high-level requirement category. The applicability of each requirement is provided in Enclosure 3 of Reference (c).
 2. A USAISEC-TIC-led CS test team conducted CS testing and published the results in a separate report, Reference (d).

LEGEND:

CR	Capability Requirements	R	Required
CS	Cybersecurity	TIC	Technology Integration Center
FR	Functional Requirements	UCR	Unified Capabilities Requirements
ID	Identification	USAISEC	U.S. Army Information Systems Engineering Command
IPv6	Internet Protocol version 6		

Table 4. DODIN APL Product Summary

Product Identification			
Product Name	ClearPass Policy Manager		
Software Release	6.9.2 (See note 1.)		
UCR Product Type(s)	NAC		
Product Description	ClearPass Policy Manager		
DODIN Certified Function	Component/ Sub-Component Name (See note 2.)	Tested Version (See note 1.)	Remarks
Network Access Device	C1000 (formerly JW770A)	6.9.2	NAC
	C2000 (formerly JX921A)		
	<u>C3000</u> (formerly JX920A)		
	C3010 (See note 3.)		
Virtual appliance	C1000V (formerly JW335AAE)	6.9.2	NAC
	C2000V (formerly JW336AAE)		
	C3000V (formerly JW337AAE)		

NOTE(S):
 1. With DTR 3, the SUT Software Release version was updated from 6.6.7 to 6.7.3. With DTR 5, the SUT Software Release version was updated from 6.7.3 to 6.9.2
 2. Components bolded and underlined were tested by USAISEC-TIC. The other components in the family series were not tested; however, JITC certified the other components for joint use because they utilize the same software and similar hardware as tested and certified components and analysis determined they were functionally identical for interoperability certification purposes.
 3. With DTR 4, the C3010 appliance by analysis and similarity to the previously certified C3000 component.

LEGEND:

APL	Approved Products List	TIC	Technology Integration Center
CS	Cybersecurity	UCR	Unified Capabilities Requirements
DODIN	Department of Defense Information Network	USAISEC	U.S. Army Information Systems Engineering Command
DTR	Desktop Review	VPN	Virtual Private Network
NAC	Network Access Device		

4. Test Details. This extension of the certification is based on DTR 5. The original certification, documented in Reference (c), was based on interoperability (IO) testing, DISA adjudication of open test discrepancy reports (TDRs), vendor's release notes, and completed Letters of Compliance (LoC) for inclusion on the DODIN APL. The United States Army Information Systems Engineering Command, Mission Engineering Directorate, Technology Integration Center (USAISEC-MED TIC), Fort Huachuca, Arizona, conducted IO testing from 14 November 2016 through 18 November 2016, using test procedures derived from Reference (e), and completed review of the Vendor's release notes and LoCs on 25 July 2017. DISA completed adjudication of outstanding TDRs on 17 January 2017. A USAISEC-TIC-led test team conducted Cybersecurity (CS) testing and published the results in a separate report, Reference (d). Enclosure 2 of Reference (c) documents the test results and describes the tested network and system configurations. Enclosure 3 of Reference (c) provides a detailed list of the interfaces and capability.

DTR 5 was requested to update the SUT Software Release version from 6.7.3 to 6.9.2.

JITC analysis, with input from USAISEC-TIC, determined no further IO or CS testing was required because the minor software update was for support of minor features and enhancements that did not change the certified IO features and functions or approved CS posture of the SUT. Furthermore, there were no past due CS or IO Vendor Plan of Action and Milestones (POA&Ms). Based on analysis, no change to the certified IO features and functions of the SUT, and no past due Vendor POA&Ms, JITC approves this DTR.

Additionally, the approved CS posture of the SUT is documented in a separate report, Reference (d).

5. Additional Information. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at <https://stp.fhu.disa.mil/>. Test reports, lessons learned, and related testing documents and references are on the JITC Industry Toolkit (JIT) at <https://jit.fhu.disa.mil/>. Due to the sensitivity of the information, the CS Assessment Package (CAP) containing the approved configuration and deployment guide must be requested directly from the Approved Products Certification Office (APCO) via e-mail: disa.meade.ie.list.approved-products-certification-office@mail.mil. All associated information is available on the DISA APCO website located at <https://aplots.disa.mil/>.

JITC Memo, JTE, Extension of the Joint Interoperability Certification of the Aruba ClearPass Policy Manager with Software Release 6.9.2

6. Point of Contact (POC). USAISEC-TIC testing POC: Ms. Michelle Lavery; commercial telephone (520) 533-3766 or DSN 312-821-3766; email address: michelle.w.lavery.civ@mail.mil. JITC certification POC: Ms. Lisa Esquivel; commercial telephone (520) 538-5531; DSN telephone 879-5531; DSN FAX: 879-4347; e-mail address: lisa.r.esquivel.civ@mail.mil; mailing address: Joint Interoperability Test Command, ATTN: JTE (Ms. Lisa Esquivel), P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The APCO tracking number for the SUT is 1608103.

FOR THE COMMANDER:

Enclosure a/s

for RIC HARRISON
Chief
Networks/Communications &
DODIN Capabilities Division

Distribution (electronic mail):

DOD CIO
Joint Staff J-6, JCS
USD (AT&L)
ISG Secretariat, DISA, JTA
US Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA (ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division
US Coast Guard, CG-64
DISA/TEMC
DIA, Office of the Acquisition Executive
NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V
HQUSAISEC, ELIE-ISE-ME
APCO

ADDITIONAL REFERENCES

- (c) Joint Interoperability Test Command Memo, JTD, "Joint Interoperability Certification of the Aruba ClearPass Policy Manager, Software Version 6.6", 09 March 2017
- (d) U.S. Army Information Systems Engineering Command, Mission Engineering Directorate, Technology Integration Center (USAISEC MED TIC), "Cybersecurity Assessment Report for Joint Interoperability Certification of the Aruba ClearPass Policy Manager, Software Version 6.9.2," October 2020
- (e) Joint Interoperability Test Command, "Unified Capabilities Security Device Test Procedures Version 1.0 for Unified Capabilities Requirements (UCR) 2013 Change 1," June 2015