Infoblox Trinzic 825, Trinzic 1425, Trinzic 2225, Trinzic 4015, and Trinzic 4025 DDI Appliances

FIPS 140-2 Non-Proprietary Security Policy

Security Level 2 Validation

Version 1.02

October 2019

Table of Contents, Table of Figures, List of Tables

Table of Contents

Table of Figures

Table of Tables

1. Overview

This document is a non-proprietary FIPS 140-2 Security Policy for Infoblox's Trinzic 825, Trinzic 1425, Trinzic 2225, Trinzic 4015 and Trinzic 4025 DDI Appliances running NIOS 8.2.6. This policy describes how these Infoblox Trinzic DDI Appliances (hereafter referred to as the "module") meet the requirements of FIPS 140-2. This document also describes how to configure the module into the FIPS 140-2 Approved mode. This document was prepared as part of a FIPS 140-2 Security Level 2 validation.

The Federal Information Processing Standards Publication 140-2 - Security Requirements for Cryptographic Modules (FIPS 140-2) details the United States Federal Government requirements for cryptographic modules. Detailed information about the FIPS 140-2 standard and validation program is available on the NIST (National Institute of Standards and Technology) website at https://csrc.nist.gov/projects/cryptographic-module-validation-program.

2. Introduction

Infoblox Trinzic 825, Trinzic 1425, Trinzic 2225, Trinzic 4015 and Trinzic 4025 DDI Appliances enable customers to deploy large, robust, manageable and cost-effective Infoblox Grids. This next-generation solution enables distributed delivery of core network services—including DNS, DHCP, IPAM, TFTP, and FTP—with the nonstop availability and real-time service management required for today's 24x7 advanced IP networks and applications. The Infoblox Trinzic 825, Trinzic 1425, Trinzic 2225, Trinzic 4015 and Trinzic 4025 DDI Appliances are being validated as a multi-chip standalone cryptographic module at FIPS 140-2 overall Security Level 2.

2.1. Infoblox Trinzic 825 DDI Appliance

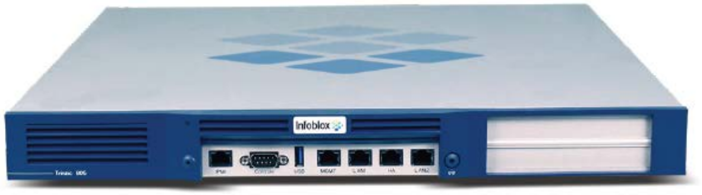


Figure 1 Trinzic 825 DDI Appliance

The Infoblox Trinzic 825 DDI Appliance is designed to serve medium and large enterprises in headquarters and regional office environments. Trinzic 825 utilizes the latest energy-efficient technology, supports a Unit Identification button/LED, and has IPMI 2.0-compliant Lights Out Management (LOM) for IPv4 for remote site management and support.

2.2. Infoblox Trinzic 1425 DDI Appliance

Figure 2 Trinzic 1425 DDI Appliance

The Infoblox Trinzic 1425 DDI Appliance is designed to serve medium and large enterprises in headquarters and regional office environments, and can be deployed as a standalone unit or in high-availability pairs. Trinzic 1425 utilizes latest energy-efficient technology, supports a Unit Identification button/LED, and has IPMI 2.0-compliant Lights Out Management (LOM) for both IPv4 and IPv6. For high availability and uptime, Trinzic 1425 supports field-replaceable hard drive and power supply, as well as optional second (redundant) power supply. Trinzic 1425 also offers a choice of AC or DC power.

2.3. Infoblox Trinzic 2225 DDI Appliance

Figure 3 Trinzic 2225 DDI Appliance[1]

The Infoblox Trinzic 2225 DDI Appliance is designed to serve medium and large enterprises in headquarters and regional office environments. Trinzic 2225 utilizes the latest energy-efficient technology, supports a Unit Identification button/LED, and has IPMI 2.0-compliant Lights Out Management (LOM) for IPv4. For high availability and uptime, Trinzic 2225 supports field-replaceable hard drive, power supply, and fans. Trinzic 2225 supports redundant power supplies and hard drives (RAID 10). Trinzic 2225 also offers a choice of AC or DC power.

[1] Note the image provided is a representative image that does not depict the tested configuration.

2.4. Infoblox Trinzic 4015 DDI Appliance

Figure 4 Trinzic 4015 DDI Appliance

The Infoblox Trinzic 4015 DDI Appliance is a high-performance, carrier-grade network appliance designed to deliver high-performance external DNS services for ISPs, telcos, and large enterprises, as well as large-scale DHCP and Grid management applications. Trinzic 4015 can be deployed standalone and in HA, as a Grid member or as a Grid master. Trinzic 4015 features redundant, hot-swappable power supplies, fan modules, and hard disk drives. Trinzic 4015 supports Unit Identification button/LEDs and Lights Out Management (LOM) and is IPMI 2.0 compliant.

2.5. Infoblox Trinzic 4025 DDI Appliance

Figure 5 Trinzic 4025 DDI Appliance

The Infoblox Trinzic 4025 DDI Appliance is a high-performance, carrier-grade network appliance designed to deliver the highest levels of scalability for the largest Grids. Trinzic 4025 contains expanded memory and processing capability to aid in managing large Grids and is designed to be used as a Grid master. Trinzic 4025 features redundant, hot-swappable power supplies, fan modules, and hard disk drives. Trinzic 4025 supports Unit Identification button/LEDs and Lights Out Management (LOM), and is IPMI 2.0 compliant.

3. Cryptographic Module Specification

3.1. Security Level Summary

The security level claimed for each section of the FIPS 140-2 standard is as follows:

Section	Title	Level
1	Cryptographic Module Specification	2

2	Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	Not Applicable
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	Not Applicable
Overall		**2**

Figure 6 Security Level Summary

3.2. Cryptographic Boundary

The cryptographic boundary for the module is the edge (front, back, left, right, top, and bottom surfaces) of the physical enclosure.

3.3. Block Diagram

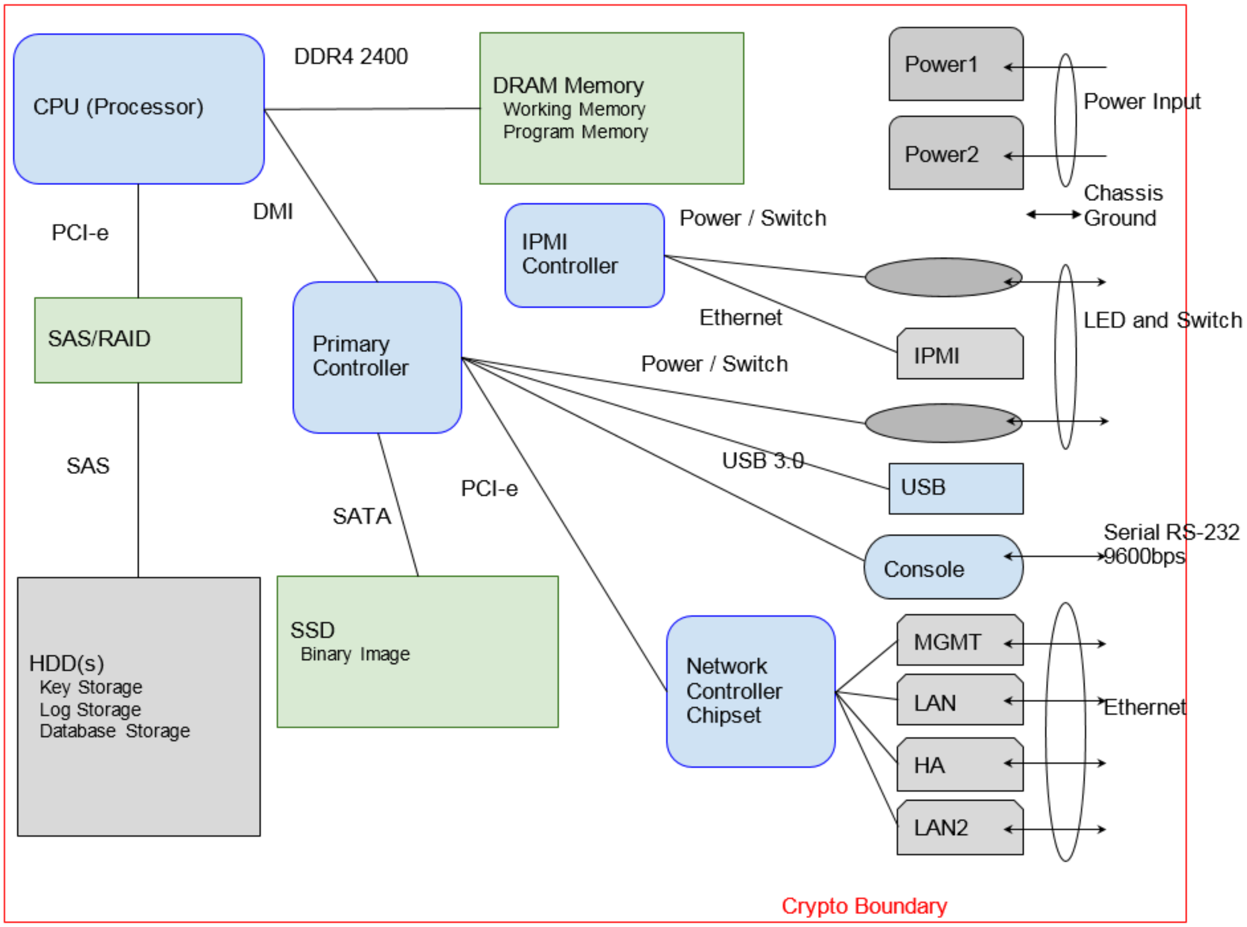


Figure 7 Block Diagram

3.4. Secure Initialization

The following steps should be followed to initialize the module into the FIPS Approved mode of operation:

- The module must be running NIOS version 8.2.6 with Hotfix-NIOS_8.2.6-371069_J67303_FIPS_2-6f0806b9bc9cbdbc9837391bb5a86a26-Tue-Aug-21-22-24-14-2018.bin2 and optionally Hotfix-NIOS_8.2.6_J69312-f7c9b7c3181ceb527aeb0aaf6536a5b3-Thu-Jan-31-06-16-41-2019.bin2
- Tamper evident labels must be applied according to Section 6.1 of this document.
- FIPS mode must be enabled in the NIOS CLI via command ‘set fips_mode’.
- The password policy must be set such that the Minimum Password Length is at least 6 characters. This can be accomplished via the procedures outlined in the Infoblox NIOS Administrator Guide, section “Managing Passwords”
- The BloxTools feature must not be enabled when operating in the FIPS Approved mode.
- The Support Access feature must not be enabled when operating in the FIPS Approved mode.
- RADIUS Authentication must not be used in the FIPS Approved mode.
- TACACS+ Authentication must not be used in the FIPS Approved mode.
- Cisco ISE Integration must not be used in the FIPS Approved mode.
- Microsoft Server Integration must not be used in the FIPS Approved mode.
- SNMPv1/v2 must not be used in the FIPS Approved mode.
- Keys/CSPs generated in FIPS mode cannot be used in non-FIPS mode and vice-versa.

Failure to follow the above procedures will result in the module operating in a non-approved mode.

3.5. Approved Algorithms

The module supports the following approved algorithms for use in the approved mode. Although the module’s cryptographic implementation supports more options than listed below, only those listed are usable by the module.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
4805	AES	FIPS 197	CBC, CBC-CS3 (vendor affirmed), CFB128	128, 256	Data Encryption / Decryption
Vendor Affirmed	CKG	SP 800-133	Section 5		Key Generation
1437	CVL (ECC CDH, KAS ECC, KAS FFC)	SP 800-56A Rev3		ECC: P-256 , P-384, P-521 FFC: 2048	Key Agreement
1438	CVL (TLS[2] 1.0/1.1/1.2, SSH SNMP)	SP 800-135 Rev1		TLS 1.2: SHA-256, SHA-384 SSH: SHA-1, SHA-256, SHA-384, SHA-	

[2] No parts of the TLS, SSH, SNMP protocols other than the KDF have been reviewed or tested by the CAVP and CMVP

				512	
1671	DRBG	SP 800-90A	HMAC-SHA-256		Deterministic Random Bit Generation
1295	DSA	FIPS 186-4		2048	FFC Key Generation[3]
1213	ECDSA	FIPS 186-4		P-256 , P-384, P-521 (w/ SHA-224, SHA-256, SHA-384, or SHA-512)	ECC Key Generation[4], Digital Signature Verification
3215	HMAC	FIPS 198-1	HMAC-SHA-1-96 HMAC-SHA-1, HMAC-SHA-256,	160, 256	Message Authentication
4805 (AES) **3215 (HMAC)**	KTS	SP 800-38F	AES-CBC, HMAC-SHA-1	AES: 128, 256 HMAC: 160	Key Transport
2633	RSA	FIPS 186-4	X9.31 PKCS1_V1_5 PSS	2048, 3072, 4096 (w/ SHA-224, SHA-256, SHA-384, or SHA-512)	Key Generation, Digital Signature Generation and Verification
3953	SHS	FIPS 180-4	SHA-1, SHA-256		Message Digest

Table 1 Approved Algorithms

3.6. Allowed Algorithms

The following algorithms are non-approved but allowed for use in the approved mode.

Algorithm	Caveat	Use
Diffie-Hellman	CVL Certs. #1437 and #1438, Key Agreement, key establishment methodology provides 112 bits of encryption strength	Key Agreement
Elliptic-Curve Diffie-Hellman	CVL Certs. #1437 and #1438, Key Agreement, key establishment methodology provides between 128 and 256 bits of encryption strength	Key Agreement
HMAC-MD5	Only allowed for use with TLS protocol.	TLS 1.0, Internals (i.e. objects comparison) HMAC for cookie.
MD5	Only allowed for use with TLS protocol.	TLS 1.0, Internals (i.e. objects comparison) HMAC for cookie.
NDRNG	This implementation satisfies scenario 1(a) of IG 7.14. The	Seeding the DRBG

[3] The FFC keys used for Diffie-Hellman are generated according to FIPS 186-4. The module does not support the generation of DSA keys with approved key sizes.

[4] The ECC keys used for EC-Diffie-Hellman are generated according to FIPS 186-4

	module obtains a minimum of 339 bits of entropy before generating keys.	
RSA	Key Wrapping, key establishment methodology provides between 112 and 150 bits of encryption strength	Key Wrapping

Table 2 Allowed Algorithms

3.7. Non-Approved Algorithms Table

The following algorithms are non-approved for use in the approved mode.

Algorithm	Caveat	Use
DES		Encryption/Decryption
Diffie-Hellman	Non-compliant when used with key sizes less than 2048 bits in length	Key Agreement
DSA		Key Generation
HMAC-MD5		Keyed Hash
MD5		Message Digest
RSA	Non-compliant when used with key sizes less than 2048 bits in length	Key Wrapping

Table 3 Non-Approved Algorithms

4. Cryptographic Module Ports and Interfaces

4.1. Logical and Physical Interfaces

The module's interfaces can be categorized under the following FIPS 140-2 logical interfaces.

- Data Input
- Data Output
- Control Input
- Status Output

The following table provides a mapping of the module's interfaces to the FIPS 140-2 defined interface categories.

Physical Interface[5]	Logical Interface(s)	Description	Notes
Network Interfaces	Data Input, Data Output, Control Input, Status Output	**Trinzic 825, 1425, 2225, 4015, and 4025**: ● Two 10/100/1000 Base-T Ethernet	LED link lights are part of status output.

[5] Although the module includes a USB port, this port is disabled and unused by the module as of the most recent FIPS 140-2 validation.

		(LAN ports) ● One 10/100/1000 Base-T Ethernet (HA port) ● One 10/100/1000 Base-T Ethernet (MGMT port)	
Serial Port	Data Input, Data Output, Control Input, Status Output	**Trinzic 825, 1425, 2225, 4015, and 4025**: ● DB-9 (9600/8n1, Xon/Xoff)	
Unit Identification	Control Input, Status Output	**Trinzic 825, 1425, 2225, 4015, and 4025**: ● Front and back	
AC Power Supply	Power Input, Status Output	**Trinzic 825**: ● Input voltage: 100–240 VAC switchable, 50–60 Hz ● Output power: 350W **Trinzic 1425**: ● One hot-swappable PSU ● Input voltage: 100–240 VAC switchable, 50–60 Hz ● Output power: 600W **Trinzic 2225, 4015, and 4025**: ● Two hot-swappable PSUs ● Input voltage: 100-240 VAC switchable, 50-60 Hz ● Output power: 600W	FIPS kit Tamper Evident Label required

DC Power Supply	Power Input, Status Output	**Trinzic 1425**: ● One hot-swappable PSU ● Input voltage: -44–65DC; 600W **Trinzic 2225, 4015, and 4025**: ● Two hot-swappable PSUs ● Input voltage: -44-65DC; 600W	FIPS kit Tamper Evident Label required
Chassis Ground	Power Input	**Trinzic 825, 1425, 2225, 4015, and 4025**: ● Included (ground lug)	
System Power Switch	Control Input	**Trinzic 825, 1425, 2225, 4015, and 4025**: ● Pin-Hole access “pc standard” Soft Power Switch	
System Power LED	Status Output	**Trinzic 825, 1425, 2225, 4015, and 4025**: ● LED indicating system power status	

Table 4 Logical and Physical Interfaces

5. Roles, Services, and Authentication

5.1. Roles

The module defines user permissions based on roles. Roles are assigned to user groups. Custom roles can be created to restrict access to particular services.

FIPS Role	Trinzic Role	Description

Crypto-Officer	Superuser	The Superuser role has full access to all resources on the appliance. Superusers can create limited-access admin groups and grant them specific permissions for Crypto Officer services.
	Limited-Access Admin	An admin belonging to a limited-access group which has been granted permissions to Crypto Officer services.
	Grid Member	A Trinzic appliance that is a member of a NIOS grid and managed by a Grid Master.
User	Limited-Access User	An admin belonging to a limited-access group which has only been granted read permissions to Grid Manager services.

5.2. Services

Listed below are the services for each of the module's roles that are approved for use in the FIPS approved mode.

Key/CSP Access is specified as:

- Generate (G) – The module generates the Key/CSP
- Read (R) – The module reads the Key/CSP
- Write (W) – The module writes/modifies the Key/CSP
- Execute (E) – The module uses the Key/CSP
- Delete (D) – The module deletes the Key/CSP

5.2.1.Crypto-Officer Services

Name	Description	Inputs	Outputs	Key/CSP Access (G/R/W/E/D)
Infoblox Console	Access NIOS CLI via console to manage appliance.	Commands and configuration data	Status of commands and configuration data	• Superuser/Admin Password (E)

Infoblox Remote Console	Access NIOS CLI via SSH to manage appliance.	SSH inputs, commands, and data	SSH outputs, commands, and data	• Superuser/Admin Password (E) • SSHv2 private key (E) • SSHv2 public key (E) • SSHv2 Diffie-Hellman Private Key (G/E/D) • SSHv2 Diffie-Hellman Public Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Private Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Public Key (G/E/D) • SSHv2 Encryption Key (G/E/D) • SSHv2 Authentication Key(G/E/D)
Infoblox Grid Manager	Access NIOS web interface to manage appliance	TLS inputs, commands, and data	TLS outputs, commands, and data	• X.509 HTTPS Certificate (E) • TLS Diffie-Hellman Private Key(G/E/D) • TLS Diffie-Hellman Public Key(G/E/D) • TLS pre-master secret (G/E/D) • TLS master secret (G/E/D) • TLS encryption key (G/E/D) • TLS authentication key (G/E/D) • Superuser/Admin Password (E) • X. 509 User Certificate (E) • X. 509 CA Certificate (E)
Show Status	View currently logged in user in Grid Manager	N/A	Status and data	None
Configure Dashboards	Home page in Grid Manager providing quick access to task, grid and network status.	Commands and configuration data	Status of commands and configuration data	None
Configure Smart Folders	Organize core networking service data in	Commands and configuration	Status of commands and	None

	Grid Manager.	data	configuration data	
Manage Licenses	Manage appliance licenses from CLI or Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Manage Users	Setting up users, groups, roles, and permissions from Grid Manager	Commands and configuration data	Status of commands and configuration data	• Superuser/Admin/User Password (W/D)
Manage Remote Authentication Services	Configure remote authentication services for Active Directory, LDAPS, or Certificate Authentication from Grid Manager.	Commands and configuration data	Status of commands and configuration data	• LDAPS Bind User Password (W/D) • X. 509 CA Certificate (R/W/D)
Deploy Grid	Creating and managing Grid master and members via Grid Manager and CLI.	OpenVPN inputs, commands, and data	OpenVPN outputs, commands, and data	• Grid Shared Secret (W/E/D) • OpenVPN TLS Public Key (E) • TLS Diffie-Hellman Private Key (G/E/D) • TLS Diffie-Hellman Public Key (G/E/D) • TLS pre-master secret (G/E/D) • TLS master secret (G/E/D) • TLS encryption key (G/E/D) • TLS authentication key (G/E/D) • OpenVPN pre-master secret (G/E/D) • OpenVPN master secret (G/E/D) • OpenVPN encryption key (G/E/D) • OpenVPN authentication key (G/E/D)

Deploy Independent appliances	Deploy Infoblox appliance as a standalone via Grid Manager and CLI.	Commands and configuration data	Status of commands and configuration data	• Superuser/Admin Password (E/D)
Deploy Cloud Network Automation	Configuring Cloud platform appliances to provide DNS and DHCP service in the cloud from Grid Manager.	Commands and configuration data	Status of commands and configuration data	None
Configure Syslog Backups	Configure Syslog to backup over FTP or SCP in Grid Manager	Commands and configuration data	Status of commands and configuration data	• SSHv2 Diffie-Hellman Private Key (G/E/D) • SSHv2 Diffie-Hellman Public Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Private Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Public Key (G/E/D) • SSHv2 Encryption Key (G/E/D) • SSHv2 Authentication Key (G/E/D)
Capture and Export Network Traffic	Capture network traffic on appliance interfaces and export capture file via SCP or TLS.	Commands and configuration data	Status of commands and configuration data	• X.509 HTTPS Certificate (E) • TLS Diffie-Hellman Private Key (G/E/D) • TLS Diffie-Hellman Public Key (G/E/D) • TLS pre-master secret (G/E/D) • TLS master secret (G/E/D) • TLS encryption key (G/E/D) • TLS authentication key (G/E/D) • SSHv2 Diffie-Hellman Private Key (G/E/D) • SSHv2 Diffie-Hellman Public Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Private Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Public Key (G/E/D)

				• SSHv2 Encryption Key (G/E/D) • SSHv2 Authentication Key (G/E/D)
Manage NTP	Manage network time protocol service in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Manage Captive Portal	Manage network captive portal in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Manage IPAM	Managing IP address management services in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Manage File Distribution Service	Managing transfer of files through TFTP, FTP and HTTP in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Managing NIOS Software and Configuration Files	Performing software upgrades and downgrades in Grid Manager. (New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and requires a separate FIPS 140-2 validation.)	Commands and configuration data	Status of commands and configuration data	• Software/Firmware Load Test Public Key (W/E)

Configure RIR Registration Updates	Managing Regional Internet Registries in Grid Manager.	Commands and configuration data	Status of commands and configuration data	None
Configure IP Address Management	Managing network and IP addresses in Grid Manager and CLI.	Commands and configuration data	Status of commands and configuration data	None
Configure IP Discovery and vDiscovery	IP discovery for detecting and obtaining information about active hosts in predefined networks in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure Infoblox Network Insight	Configure united network discovery for geographically dispersed networks in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure DNS	Configuring DNS services in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure DNSSEC	Configure DNSSEC services in Grid Manager	Commands and configuration data	Status of commands and configuration data	• DNSSEC KSK Private Key (G/E/D) • DNSSEC KSK Public Key (G/W/E/D) • DNSSEC ZSK Private Key (G/W/E/D) • DNSSEC ZSK Public Key (G/W/E/D)
Configure DHCP	Configuring DHCP services in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure Authenticated DHCP	Configure DHCP to authenticate users using configured	Commands and configuration data	Status of commands and configuration data	None

	Remote Authentication servers in Grid Manager			
Configure Appliance Monitoring	Configure monitoring state of appliance, service, database capacity, and ports in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure DHCP Fingerprint Detection	DHCP fingerprint detection to identify IPv4 and IPv6 devices in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure SNMPv3	Configure SNMPv3 in Grid Manager	Commands and configuration data	Status of commands and configuration data	• SNMPv3 Auth Password (W/D) • SNMPv3 Privacy Password (W/D)
Configure Infoblox Reporting and Analytics	Configure automated collection, analysis and presentation of core networking data in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure Infoblox Advanced DNS protection	Configure threat protection rules to detect, report and stop DoS, DDoS and other network attacks targeting DNS in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure Infoblox DNS Firewall	Configure DNS Resource policy zones to	Commands and configuration	Status of commands and	None

	control DNS lookups in Grid Manager	data	configuration data	
Configure Infoblox Threat Insight	Configure for protecting mission critical DNS infrastructure in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure Ecosystem – Outbound Notifications	Using RESTful API and DXL for obtaining core network service information	Commands and configuration data	Status of commands and configuration data	• X.509 HTTPS Certificate (E) • TLS Diffie-Hellman Private Key (G/E/D) • TLS Diffie-Hellman Public Key (G/E/D) • TLS pre-master secret (G/E/D) • TLS master secret (G/E/D) • TLS encryption key (G/E/D) • TLS authentication key (G/E/D) • Superuser/Admin Password (E) • X. 509 User Certificate (E) • X. 509 CA Certificate (E)
Configure Informational GUI Banner	Configure informational banner to display in Grid Manager	Commands and configuration data	Status of commands and configuration data	None
Configure Dynamic DNS Services	Configure Kerberos Authenticated Dynamic DNS services in Grid Manager	Commands and configuration data	Status of commands and configuration data	• GSS-TSIG Encryption Key (W/D) • GSS-TSIG Authentication Key (W/D)
Zeroization	Zeroize all keys/CSPs	Commands and configuration data	Status of commands and configuration data	All (D)

Table 5 Crypto-Officer Services

5.2.2.User Services

Name	Description	Inputs	Outputs	Key/CSP Access
Authenticated DHCP	Authenticate to DHCP server via Remote Access Server	Remote authentication inputs and data.	Status and Client network configuration	• User Password (E) • LDAPS Bind User Password (E) • X. 509 CA Certificate (E)
Infoblox Grid Manager	Access NIOS web interface over TLS.	TLS inputs, commands, and data	TLS outputs, commands, and data	• X.509 HTTPS Certificate (E) • TLS Diffie-Hellman Private Key (G/E/D) • TLS Diffie-Hellman Public Key (G/E/D) • TLS pre-master secret (G/E/D) • TLS master secret (G/E/D) • TLS encryption key (G/E/D) • TLS authentication key (G/E/D) • Superuser/Admin Password (E) • X. 509 User Certificate (E) • X. 509 CA Certificate (E)
Show Status	View currently logged in user in Grid Manager	N/A	Status and data	None
Change User Password	Change password of currently authenticated user	Commands and configuration data	Command status and data	• User Password (W/D)
Configure Dashboards	Configure home page in Grid Manager providing quick access to task, grid and network status.	Commands and configuration data	Status and data	None
View Dashboards	Home page in Grid Manager providing quick access to task, grid and network status.	Commands and data	Status and data	None

Access Smart Folders	Organize core networking service data in Grid Manager.	Commands and data	Status and data	None
View Licenses	View appliance licenses from Grid Manager	Commands and data	Status and data	None
View and Export Log Files	View and export log files from Grid Manager.	Commands and data	Status and data	• X.509 HTTPS Certificate (E) • TLS Diffie-Hellman Private Key (G/E/D) • TLS Diffie-Hellman Public Key (G/E/D) • TLS pre-master secret (G/E/D) • TLS master secret (G/E/D) • TLS encryption key (G/E/D) • TLS authentication key (G/E/D) • SSHv2 Diffie-Hellman Private Key (G/E/D) • SSHv2 Diffie-Hellman Public Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Private Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Public Key (G/E/D) • SSHv2 Encryption Key (G/E/D) SSHv2 Authentication Key (G/E/D)
Capture and Export Network Traffic	Capture network traffic on appliance interfaces and export capture file via SCP or TLS.	Commands and data	Status and data	• X.509 HTTPS Certificate (E) • TLS Diffie-Hellman Private Key (G/E/D) • TLS Diffie-Hellman Public Key (G/E/D) • TLS pre-master secret (G/E/D) • TLS master secret (G/E/D) • TLS encryption key (G/E/D) • TLS authentication key (G/E/D)

				• SSHv2 Diffie-Hellman Private Key (G/E/D) • SSHv2 Diffie-Hellman Public Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Private Key (G/E/D) • SSHv2 Elliptic-Curve Diffie-Hellman Public Key (G/E/D) • SSHv2 Encryption Key (G/E/D) • SSHv2 Authentication Key (G/E/D)
SNMPv3	Send SNMPv3 traps	SNMPv3 inputs, commands, and data	SNMPv3 outputs, status, and data	• SNMPv3 encryption key (G/E/D) • SNMPv3 authentication key (G/E/D)
Infoblox Reporting and Analytics	Collect automated collection, analysis and presentation of core networking data.	Commands and data	Status and data	None
Ecosystem – Outbound Notifications	Using RESTful API and DXL for obtaining core network service information	TLS inputs, commands, and data	TLS outputs, status, and data	• X.509 HTTPS Certificate (E) • TLS Diffie-Hellman Private Key (G/E/D) • TLS Diffie-Hellman Public Key (G/E/D) • TLS pre-master secret (G/E/D) • TLS master secret (G/E/D) • TLS encryption key (G/E/D) • TLS authentication key (G/E/D) • Superuser/Admin Password (E) • X. 509 User Certificate (E) • X. 509 CA Certificate (E)

Table 6 User Services

5.2.3.Unauthenticated Services

Name	Description	Inputs	Outputs

Captive Portal	Access captive portal.	Commands and data	Command status and data
DNS	Domain Name Service queries.	Commands and data	Command status and data
DHCP	Receive network configuration from appliance DHCP server.	Commands and data	Command status and data
File Distribution Service	Appliance hosted FTP, TFTP, or HTTP file distribution service. *Cannot be used to distribute keys or CSPs.	Commands and data	Command status and data
NTP	Receive network time protocol updates from appliance NTP service.	Commands and data	Command status and data
View Console Status	DB-9 Console Output.	None	Status and data
On-Demand Self-Tests	On-demand self-tests invoked by rebooting the module.	None	Status and data

Table 7 Unauthenticated Services

5.2.4.Non-Approved Services

The following services are non-approved for use in the FIPS approved mode.

Name	Description
Support Access	Support Access SSH service
bloxTools	Pre-installed environment to host custom web based applications

RADIUS Authentication	Remote user authentication using RADIUS protocol
TACACS+ Authentication	Remote user authentication using TACACS+ protocol
Cisco ISE Integration	Authenticating to Cisco Identity Services Engine
Microsoft Server Integration	Managing Microsoft DNS/DHCP servers using BIND
SNMPv1/v2	Simple Network Management Protocol versions 1 and 2

Table 8 Non-approved Services

5.3. Authentication

The module has the following methods of role based authentication:

- **Local password-based authentication**
- **Remote password-based authentication** (Active Directory, LDAPS)
- **Certificate authentication**
- **Two-Factor authentication**
- **Grid Member Challenge-response authentication mechanism**

Assuming that the Secure Initialization routine is followed, Infoblox enforces a 6 character minimum password, using a 72 character set of **a-z**, **A-Z**, **0-9**, and “**!@#%^&*()**”. This results in a bare minimum of 139,314,069,504 (72^6) possible passwords. Thus the FIPS 140-2 requirement that for a single random password attempt the probability of success must be less than 1 in 1,000,000 is satisfied.

FIPS 140-2 requires that in a 1-minute span, the probability of guessing the password correct (at random) must be less than 1 in 100,000.

The web interface only allows 5 unsuccessful login attempts per minute. This calculates to a 1 in 27,862,813,900.8 ((72^6)/5) chance of a successful password attempt in a minute, which is less than the 1 in 100,000 requirement.

The SSH interface implements a maximum of 3 tries per login attempt with each failed attempt adding an incremented delay of 5 seconds. 3 failed attempts will take 30 seconds (5 + 10 + 15), therefore, in 1 minute only 6 attempts can be made. This calculates to a 1 in 23,219,011,584 ((72^6)/6) chance of a successful password attempt in a minute, which is less than the 1 in 100,000 requirement.

The console interface implements a delay of three seconds per invalid login attempt. As such, a maximum of 20 invalid login attempts are possible per minute. This calculates to a 1 in 6965703475.2 ((72^6)/20) chance of a successful password attempt in a minute, which is less than the 1 in 100,000 requirement.

Two-Factor authentication (Password + X.509 certificate authentication)

If Two-Factor authentication is used, the calculations are based on the security-strength of the algorithm. For example, if the X.509 certificate is RSA-2048 w/ SHA-256, then the security-strength is 112 bits (based on SP 800-57). Based on this, a 1 in 2^112 chance is much less than 1 in 1,000,000 per single attempt. With the worst case assumption that the network interface can support up to 29,296,875 ((1,000,000,000 bps / 2048 bits) * 60 seconds) connection attempts per minute. The chance of a successful authentication attempt in a minute calculates to a (2^112)/29,296,875, which satisfies the 1 in 100,000 requirement.

Infoblox Two-Factor authentication provides option 'Username/password request'. If you select this option NIOS populates the username from the certificate and requests password from the user. If you do not select this option, only the certificate is necessary to log in to the appliance.

NIOS performs lookup against local users by default. You can enable remote lookup for user membership (Active Directory or LDAPS). A password must not be empty.

Certificates are validated by an OCSP responder.

Grid Member Challenge-response authentication mechanism

The grid member login handshake consists of an initial 3-way authentication mechanism:

1. Challenge [replica -> master] A challenge comprising time and random data and a hash of that and the shared secret is sent.
2. Response challenge [master -> replica] A response comprising a SHA256 hash of the challenge from Item1 and the shared secret is returned along with a challenge comprising time and random data.
3. Response request [replica -> master] A response comprising a SHA256 hash of the challenge from Item 2 and the shared secret and grid name is sent.

At this point, a secure VPN tunnel is created between the replica and master. Lower bounds on the shared secret length and required entropy are listed elsewhere as 72^6. A failed connection attempt must wait 30 seconds for the clusterd state machine to time out. This clearly meets the 1 in 100,000 requirement.

6. Physical Security

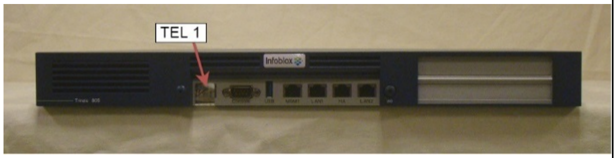
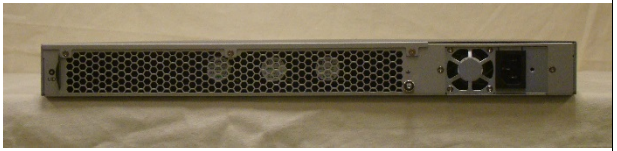
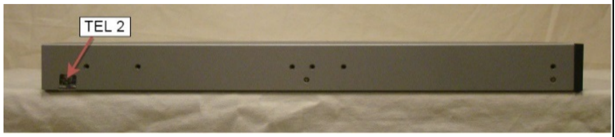
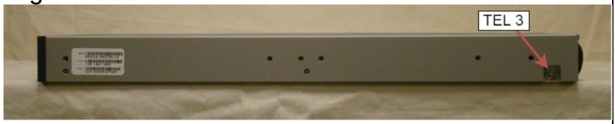
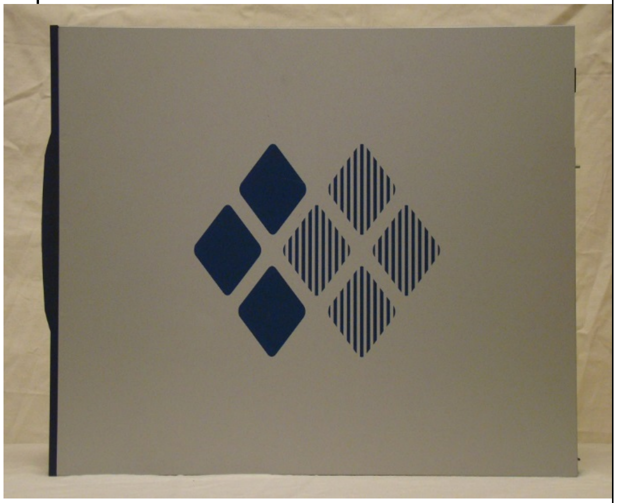
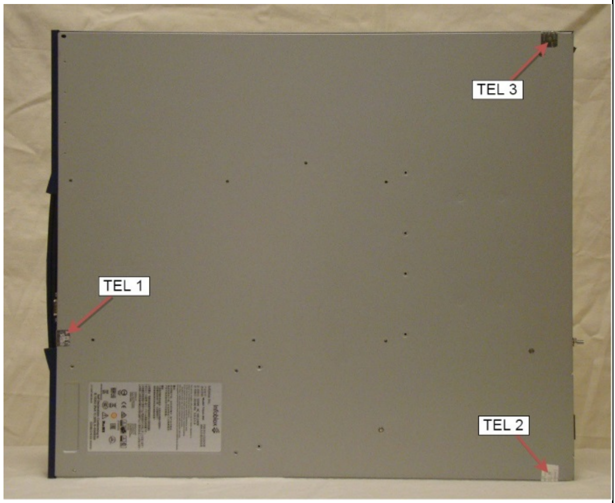
The module must be opaque within the visible spectrum and have tamper evident labels for doors or removable covers in order to be compliant with FIPS 140-2 Security Level 2 requirements. Infoblox provides tamper evident labels (TELs) which must be installed for the module to operate in the FIPS approved mode. The Crypto Officer is responsible for inspecting the TELs regularly[6] for signs of tamper, and should contact Infoblox customer support if any signs of tamper are found.

Label Kit – Description	**Label Kit - Part Number**
Infoblox Tamper Evident Seal Kit	IB-FIPS

Table 9 Tamper Evident Labels

6.1. Tamper Evident Label Placement

The tamper evident labels must be affixed to the module by the Crypto Officer at the following locations after ensuring the applying surface is clean.

Infoblox Trinzic 825 Tamper Evident Label Placement (3 labels)	
Front  	Rear 
Left  	Right 
Top 	Bottom 

[6] The inspection interval for the TELs is at the discretion of the Crypto Officer, and their standard operating procedures.

Table 10 Infoblox Trinzic 825 Tamper Evident Label Placement

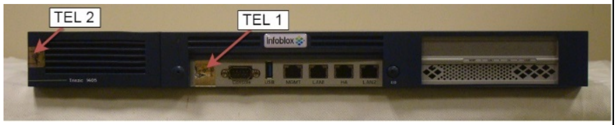
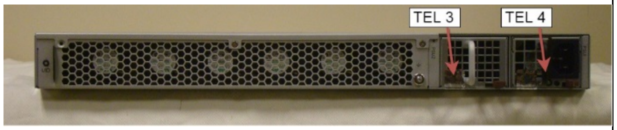
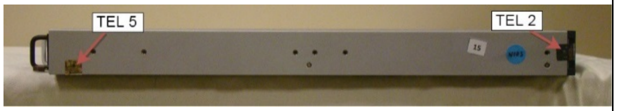
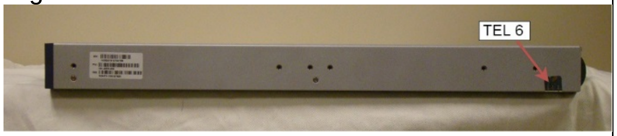
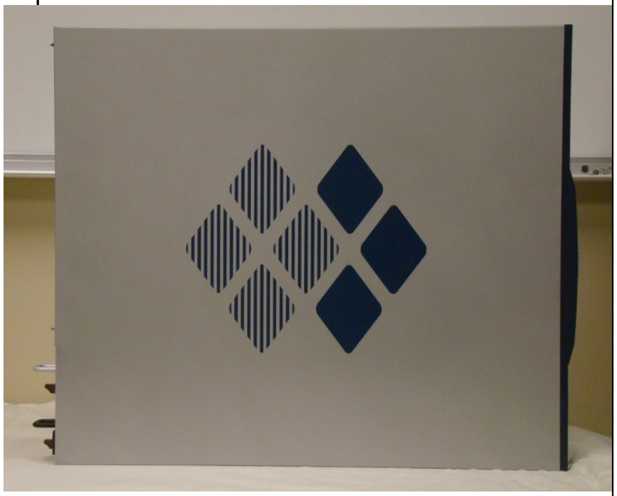
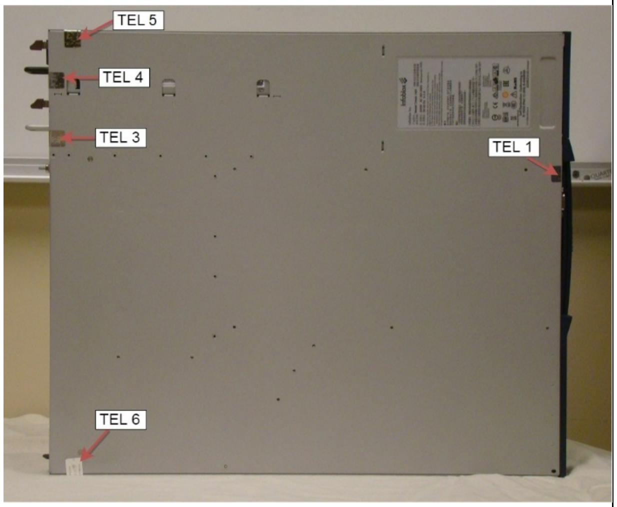
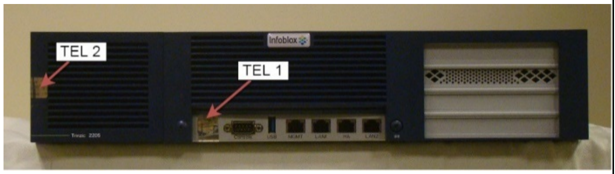
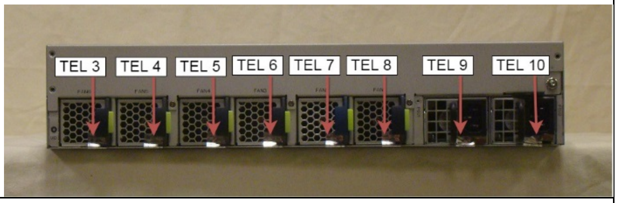
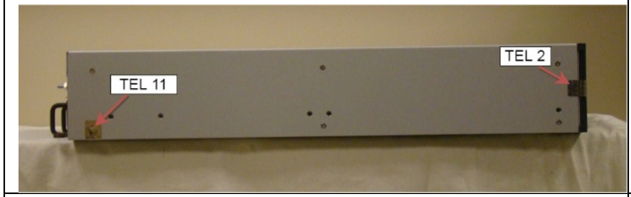
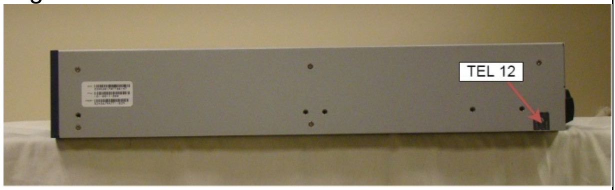
Infoblox Trinzic 1425 Tamper Evident Label Placement (6 labels)	
Front  	Rear 
Left  	Right 
Top 	Bottom 

Table 11 Infoblox Trinzic 1425 Tamper Evident Label Placement

Infoblox Trinzic 2225, 4015, and 4025 Tamper Evident Label Placement (12 labels)	
Front  	Rear  TEL 3 TEL 4 TEL 5 TEL 6 TEL 7 TEL 8 TEL 9 TEL 10
Left  	Right 
Top	Bottom

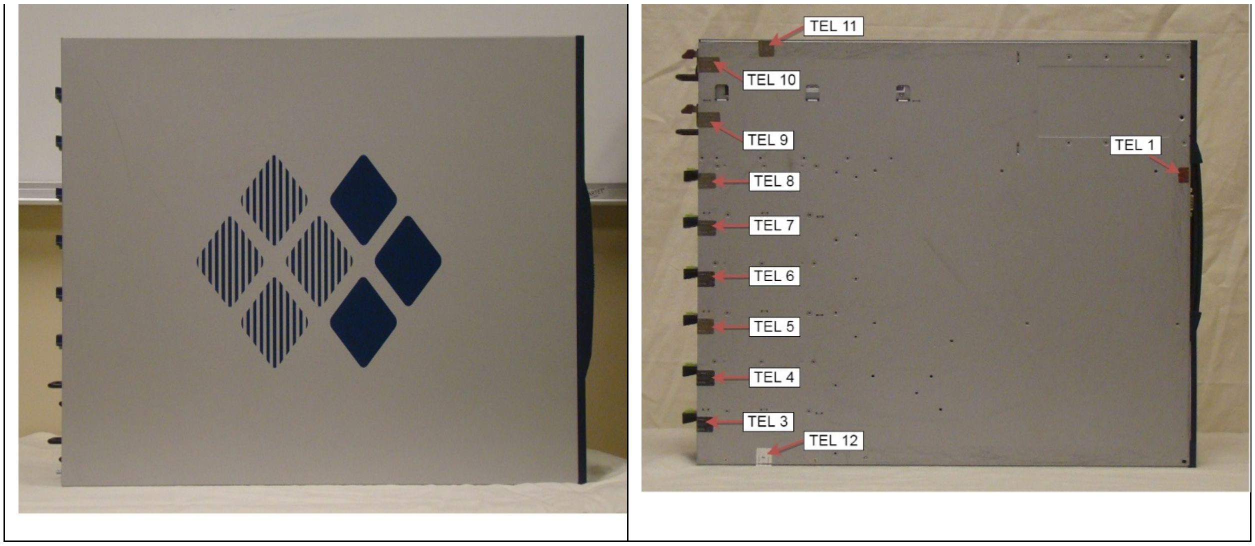


Table 12 Infoblox Trinzic 2225, 4015, and 4025 Tamper Evident Label Placement

7. Operational Environment

The module is a multi-chip standalone hardware module operating with a non-modifiable operational environment.

8. Cryptographic Key Management

Key/CSP Name	Key/CSP Type	Key/CSP Size	Generation/ Input[7]	Output	Storage	Zeroization	Use[8]
Superuser / Admin / User Password	Password	6 (or more) characters, **a-z**, **A-Z**, **0-9**, or “**!@#%^&*()**”	Input into module encrypted (via SSH or TLS)	N/A	The password is stored in the module’s persistent memory (DB)	Via zeroization service.	Authentication for Superuser, Limited-Access Admin, or User
LDAPS Bind User Password	Password	6 (or more) characters, **a-z**, **A-Z**, **0-9**, or “**!@#%^&*()**”	Input into module encrypted (via TLS)	N/A	The password is stored in the module’s persistent memory (DB)	Via zeroization service.	Authentication for credential for remote LDAPS server.
Integrity Test Public Key	RSA Public Key (with SHA256 Signature Algorithm)	4096 bits	Generated internally.	N/A	Stored in the module’s persistent memory	Via zeroization service.	Integrity Test

[7] For all keys marked as “generated internally”, the resulting symmetric key or the generated seed to be used in the asymmetric key generation is an unmodified output from the DRBG unless otherwise noted.

[8] Keys/CSPs generated in FIPS mode cannot be used in non-FIPS mode and vice-versa.

Integrity Test Private Key	RSA Private Key	4096 bits	Generated internally.	N/A	Stored in the module’s persistent memory	Via zeroization service.	Integrity Test
Software / Firmware Load Test Public Key	RSA Public Key (with SHA256 Signature Algorithm)	2048 bits	This key is not generated by the module.	N/A	This key is hard-coded into the module; stored in the module’s persistent memory.	N/A	Software / Firmware Load Test
X.509 CA Certificate	x.509 Certificate with ECDSA, or RSA Public Key (with SHA-224, SHA-256, SHA-384, or SHA-512 Signature Algorithm)	ECDSA: P-256 (256 bits), P-384 (384 bits), P-521 (521 bits) RSA: 2048 bits, 3072 bits, 4096 bits	Generated Externally	Encrypted (via TLS)	Stored in the module’s persistent memory (DB)	Via zeroization service.	External Trusted CA Certificate
X.509 HTTPS Certificate	X.509 Certificate with RSA Public Key (with SHA-256 Signature Algorithm)	2048 bits, 4096 bits	Generated internally, or input into module encrypted (via TLS)	Encrypted (via TLS)	Stored in the module’s persistent memory (DB)	Via zeroization service.	HTTPS Server Certificate
X.509 HTTPS Certificate Private Key	RSA	2048 bits, 4096 bits	Generated Internally	N/A	Stored in the module’s persistent memory (DB)	Via zeroization service.	Private key for HTTPS Server Certificate
X. 509 Client Certificate	X.509 Certificate with RSA Public Key (with SHA-256 Signature Algorithm)	2048 bits	Generated Internally	Encrypted (via TLS)	Stored in the module’s persistent memory (DB)	Via zeroization service.	Authenticating the Module to an external server.
X. 509 Client Certificate Private Key	RSA	2048 bits	Generated Internally	N/A	Stored in the module’s persistent memory (DB)	Via zeroization service.	Private Key for Client Certificate

X. 509 User Certificate	X.509 Certificate with RSA Public Key (with SHA-256 or SHA-512 Signature Algorithm)	2048 bits 3072 bits 4096 bits	Generate Externally	Plaintext	Stored in the module's dynamic memory	After user is authenticated	Authenticate user to module.
SSHv2 Private Key	RSA	2048 bits	Generated internally	N/A	Stored in the module's persistent memory.	Upon session re-key or termination.	This is the private host key used for SSHv2 authentication
SSHv2 Public Key	RSA	2048 bits	Generated internally	Plaintext	Stored in the module's persistent memory.	Via zeroization service.	This is the public host key used for SSHv2 authentication
SSHv2 Diffie-Hellman Private Key	Diffie-Hellman	2048 bits	Generated internally	N/A	Stored in dynamic memory.	Upon negotiation of shared secret	SSH Key Agreement
SSHv2 Diffie-Hellman Public Key	Diffie-Hellman	2048 bits	Generated internally	Plaintext	Stored in dynamic memory	Upon negotiation of shared secret	SSH Key Agreement
SSHv2 Elliptic-Curve Diffie-Hellman Private Key	Elliptic-Curve Diffie-Hellman	256 bits, 384 bits, 521 bits	Generated internally	N/A	Stored in dynamic memory	Upon negotiation of shared secret	SSH Key Agreement
SSHv2 Elliptic-Curve Diffie-Hellman Public Key	Elliptic-Curve Diffie-Hellman	P-256 (256 bits), P-384 (384 bits), P-521 (521 bits)	Generated internally	Plaintext	Stored in dynamic memory	Upon negotiation of shared secret	SSH Key Agreement
SSHv2 Encryption Key	AES-128-CBC, AES-256-CBC	128 bits, 256 bits	Derived via the SP800-135 KDF	N/A	Ephemeral	Upon session re-key or termination.	This is the SSHv2 session key; used to encrypt SSHv2 data traffic

SSHv2 Authentication Key	HMAC-SHA1	160 bits	Derived via the SP800-135 KDF	N/A	Ephemeral	Upon session re-key or termination.	This is the SSHv2 authentication key; used to authenticate SSHv2 data traffic
snmpEngine ID	Unique ID	32-byte maximum length	Generated externally	Plaintext	Hardcoded, stored in the module’s persistent memory.	N/A	This is the SnmpEngineID as defined in RFC3411, used to identify the SNMP engine
SNMPv3 Auth Password	Password	6 (or more) characters, **a-z**, **A-Z**, **0-9**, or “**!@#%^&*()**”	Input into module encrypted (via SSH or TLS)	N/A	This password is stored in the module’s persistent memory (DB) in AES encrypted form	Via zeroization service.	Authentication for SNMPv3
SNMPv3 Privacy Password	Password	6 (or more) characters, **a-z**, **A-Z**, **0-9**, or “**!@#%^&*()**”	Input into module encrypted (via SSH or TLS)	N/A	This password is stored in the module’s persistent memory (DB) in AES encrypted form	Via zeroization service.	Privacy for SNMPv3
SNMPv3 Encryption Key	AES-128 CFB	128 bits	Derived via the SP800-135 KDF	N/A	Ephemeral	Upon session re-key or termination.	Encryption for SNMPv3
SNMPv3 Authentication Key	HMAC-SHA-1-96	160 bits	Derived via the SP800-135 KDF	N/A	Ephemeral	Upon session re-key or termination.	Encryption for SNMPv3
TLS Diffie-Hellman Private Key	Diffie-Hellman	2048 bits	Generated internally	N/A	Stored in dynamic memory.	Upon negotiation of shared secret	TLS Key Agreement
TLS Diffie-Hellman Public Key	Diffie-Hellman	2048 bits	Generated internally	Plaintext	Stored in dynamic memory	Upon negotiation of shared secret	TLS Key Agreement
TLS Pre-master Secret	Key Material	384 bits (RSA Key Transport), 2048 bits	Entered into the module protected by RSA, or derived via	N/A	Ephemeral	Upon completion of key derivation.	Used to derive TLS master secret

		(Diffie-Hellman Key Agreement)	Diffie-Hellman				
TLS Master Secret	Key Material	48 bytes (384 bits)	Derived from pre-master secret	N/A	Ephemeral	Upon completion of key derivation.	Used to produce keys in TLS handshake
TLS Encryption Key	AES-128 CBC, AES-256 CBC	128 bits, 256 bits	Derived via the SP800-135 KDF	N/A	Ephemeral	Upon session re-key or termination.	Used to encrypt traffic in TLS
TLS Authentication Key	HMAC-SHA-1	160 bits	Derived via the SP800-135 KDF	N/A	Ephemeral	Upon session re-key or termination.	Used to authenticate traffic in TLS
OpenVPN TLS Private Key	RSA Private Key	2048-bits	Generated externally. Input encrypted (via TLS)	N/A	This key is stored in the module's persistent memory	Via zeroization service.	Used for TLS in OpenVPN to authenticate NIOS appliance.
OpenVPN TLS Public Key	RSA Public Key	2048-bits	Generated externally. Input encrypted (via TLS)	N/A	This key is stored in the module's persistent memory	Via zeroization service.	Used for TLS in OpenVPN to authenticate NIOS appliance.
OpenVPN Pre-master Secret	Key Material	48 bytes (384 bits)	Derived via Diffie-Hellman	N/A	Ephemeral	Upon completion of key derivation.	Used to produce keys in an OpenVPN TLS handshake
OpenVPN Master Secret	Key Material	48 bytes (384 bits)	Derived from pre-master secret	N/A	Ephemeral	Upon completion of key derivation.	Used to produce keys in OpenVPN TLS handshake
OpenVPN Encryption Key	AES-256 CBC	256 bits	Derived via the SP800-135 KDF	N/A	Ephemeral	Upon session re-key or termination.	Used to encrypt traffic in OpenVPN

OpenVPN Authentication Key	HMAC-SHA-1	160 bits	Derived via the SP800-135 KDF	N/A	Ephemeral	Upon session re-key or termination.	Used to authenticate traffic in OpenVPN
Grid Shared Secret	Shared Secret used in HMAC-SHA-256 CRAM authentication	6 (or more) characters, **a-z**, **A-Z**, **0-9**, or “**!@#%^&*()**”	Input into module encrypted (via SSH or TLS)	N/A	Shared Secret is stored in the module’s persistent memory (DB) in AES encrypted form	Via zeroization service.	Used to authenticate Grid members when establishing a VPN tunnel
DNSSEC KSK Private Key	RSA Private Key	2048 bits, 3072 bits, 4096 bits	Generated Internally	N/A	Stored in persistent memory	Via zeroization service.	Used to sign all DNSKEY records
DNSSEC KSK Public Key	RSA Public Key (with SHA-256 or SHA-512 signatures)	2048 bits, 3072 bits, 4096 bits	Generated Internally	Plaintext	Stored in persistent memory	Via zeroization service.	Used to sign all DNSKEY records
DNSSEC ZSK Private Key	RSA Private Key	2048 bits, 3072 bits, 4096 bits	Generated Internally	N/A	Stored in persistent memory	Via zeroization service.	Used to sign each RRset in a zone
DNSSEC ZSK Public Key	RSA Public Key (with SHA-256 or SHA-512 signatures)	2048 bits, 3072 bits, 4096 bits	Generated Internally	Plaintext	Stored in persistent memory	Via zeroization service.	Used to sign each RRset in a zone
HMAC DRBG entropy input	256-bit Entropy Input during regular run, 320-bytes - during instantiate phase		Generated by the module’s NDRNG	N/A	Ephemeral	Upon reseed and shutdown.	Random Number Generation
HMAC DRBG seed	Seed	440-bits	Derived via the SP800-90A Mechanisms	N/A	Ephemeral	Upon reseed and shutdown.	DRBG Seed
HMAC DRBG V	Internal State Value	256 bits	Derived via the SP800-90A Mechanisms	N/A	Ephemeral	Upon reseed and shutdown.	DRBG Internal State

HMAC DRBG Key	Internal State Value	256 bits	Derived via the SP800-90A Mechanisms	N/A	Ephemeral	Upon reseed and shutdown.	Random Number Generation
GSS-TSIG Encryption Key	AES-128-CTS, AES-256-CTS Kerberos Key	128 bits, 256 bits	Generated externally. Input into module encrypted (via TLS)	Output encrypted (via TLS)	Stored encrypted in persistent memory.	Via zeroization service.	Used for Secure DDNS Updates
GSS-TSIG Authentication Key	HMAC-SHA-1-96 Kerberos Key	160 bits	Generated externally. Input into module encrypted (via TLS)	Output encrypted (via TLS)	Stored encrypted in persistent memory.	Via zeroization service.	Used for Secure DDNS Updates
Key Encryption Key (KEK)	AES-128-CBC key	128 bits	Generated internally	N/A	Stored in persistent memory.	Via zeroization service.	Used for encrypting database keys.

Table 13 Cryptographic Keys and CSPs

9. Self-Tests

Output via the Data Output interface is inhibited during the performance of self-tests. The module enters the error state upon any self-test failure. The following self-tests are executed automatically without any need for input or actions from the user.

9.1. Power-on Self-Tests

The results of the power-on self-tests are output via the console and to the system syslog.

- Integrity Test
- SHA-1 Known Answer Test
- HMAC-SHA-1/256/384/512 Known Answer Tests
- AES ECB encrypt / decrypt Known Answer Test
- RSA sign / verify Known Answer Test
- ECDSA sign / verify Known Answer Test
- HMAC_DRBG w/ SHA-256 Known Answer Tests (Instantiate, Reseed, Generate)
- Primitive “Z” Computation Known Answer Test for Diffie-Hellman
- Primitive “Z” Computation Known Answer Test for Elliptic-Curve Diffie-Hellman

9.2. Conditional Self-Tests

- Continuous Random Number Generator Test (CRNGT) on the SP800-90A HMAC_DRBG w/ SHA-256
- Health Tests (Instantiate, Reseed, Generate) on the SP800-90A HMAC_DRBG w/ SHA-256
- SP800-90B Health Tests (Repetition Count Test and Adaptive Proportion Test) for the NDRNG
- ECDSA Pair-wise Consistency Test
- RSA Pair-wise Consistency Test
- Diffie-Hellman Pair-wise Conditional Test
- Elliptic-Curve Diffie-Hellman Pair-wise Conditional Test

- Conditional Tests for Assurances (as specified in SP800-56A Sections 5.5.2, 5.6.2 and 5.6.3)
- Firmware Load Test

9.3. Critical Functions Tests

- Memory test – All memory is tested and isolated faulty memory is disabled

A. Appendices

Table of Acronyms:

Acronym	Definition
8N1	Eight Data Bits, No Parity Bit, One Stop Bit
AC	Alternating Current
AES	Advanced Encryption Standard
CA	Certificate Authority
CVL	Component Validation List
DB9/DB-9	D-Subminiature 9
DC	Direct Current
DDI	DNS, DHCP, and IPAM
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DTC	DNS Traffic Control
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
HA	High Availability
HMAC	Hash-based Message Authentication Code
HSM	Hardware Security Module
IKE	Internet Key Exchange
IP	Internet Protocol
IPAM	Internet Protocol Address Management
IPMI	Intelligent Platform Management Interface
IPsec	Internet Protocol Security
KAS	Key Agreement Scheme
KDF	Key Derivation Function
LAN	Local Area Network
LBDN	Load Balanced Domain Name
LDAP	Lightweight Directory Access Protocol
LCD	Liquid-Crystal Display
LOM	Lights-Out Management
MAC	Media Access Control
MD5	Message Digest 5
MGMT	Management
NEBS	Network Equipment-Building System
NDRNG	Non-Deterministic Random Number Generator
PKI	Public Key Infrastructure
PRNG	Pseudo-Random Number Generator
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial-In User Service
RAID	Redundant Array of Independent Disks
RC4	Rivest Cipher 4
RSA	Rivest, Shamir and Adleman (cryptosystem)
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMP	Simple Network Management Protocol
SSH	Secure Shell

TACACS+	Terminal Access Controller Access-Control System
TLS	Transport Layer Security
TFTP	Trivial File Transfer Protocol
USB	Universal Serial Bus
VAC	Voltage in Alternating Current
XOFF	Pause Transmission
XON	Resume Transmission

Corporate Headquarters: +1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com