Infoblox Trinzic Appliances with NIOS 7.1

Common Criteria Security Target

Document Version: 2.3

December 2015

Prepared For:
Infoblox
3111 Coronado Drive
Santa Clara, CA 95054

Prepared By:
CSC
7231 Parkway Drive
Hanover, MD 21076

This page is intentionally blank.

Table of Contents

List of Tables

1 Security Target Introduction

This Chapter presents Security Target (ST) identification information and an overview of the ST. An ST contains the information technology (IT) security requirements of an identified Target of Evaluation (TOE) and specifies the functional and assurance security measures offered by that TOE to meet stated requirements. The Security Target contains the following sections:

- Security Target Introduction [Section 1]
- Conformance Claims [Section 2]
- Security Problem Definition [Section 3]
- Security Objectives [Section 4]
- IT Security Requirements [Section 5]
- TOE Summary Specification [Section 6]

The structure and content of this ST comply with the requirements specified in the Common Criteria (CC), Part 1, Annex A.

1.1 ST and TOE Reference

This section provides information needed to identify and control this ST and its associated TOE.

ST Title:	Infoblox Trinzic Appliances with NIOS 7.1 Security Target
ST Version:	2.3
Publication Date:	December, 2015
Authors:	CSC Security Testing and Certification Laboratories, Infoblox
TOE Identification:	Infoblox ND-800, TR-800, TE-810, TE-820, TR-1400, TE-1410, TE-1420, PT-1400, ND-1400, TR-2200, TE-2210, TE- 2220, PT-2200, ND-2200, TR-4000, IB-4010, IB-4020, PT-4000, PT-4000-10G, IB-4030, IB-4030-10G, ND-4000 with NIOS Version 7.1
Keywords:	network device, secure DNS, DHCP, IP Address Management (IPAM)

1.2 TOE Overview

The TOE, i.e. ND-800, TR-800, TE-810, TE-820, ND-800, TR-1400, ND-1400, TE-1410, TE-1410, TE-1420, ND-2200, TR-2200, TE-2210, TE-2220, ND-4000, TR-4000, IB-4010, IB-4020, IB-4030, PT-1400, PT-2200, PT-4000, and PT-4000-10GE with NIOS/IBOS Version 7.1 (hereafter referred to as Infoblox Appliances), are network appliances which provide delivery of IP network services and management , including DNS, DHCP, IPAM, FTP, TFTP, and HTTP.

The NIOS operating system is a hardened version of the Fedora Linux distribution optimized for security and network performance. The appliance models are differentiated by performance, capacity and availability to support various deployment scenarios such as a branch-office or large enterprise.

The TOE provides the following major security features:

- **Secure management.** Administrators manage the TOE via a TLS protected web GUI or via the CLI console port. The TOE implements role based access control, password based authentication and auditing of management functions. Communication with the TOE's API interface is protected by TLS.
- **High availability.** The TOE enforces quotas on exhaustible resources thereby preventing failover due to resource exhaustion.
- **Trusted updates.** The TOE uses digital signatures to verify updates prior to installation.
- **Self protection.** The TOE performs self-test at startup to verify the integrity of hardware components and the cryptographic module.

The Infoblox Trinzic Appliances within the scope of evaluation are shown in Table 1 .

Table 1: TOE Models

Infoblox Model	CPU	CPU Speed	Memory	Storage[1]	Network Connectivity
ND-800	Intel Pentium G6950	1.6 GHz	8GB	500GB	4x1GBe Ethernet, nonaccelerated
TR-800	Intel Pentium G6950	1.2 GHz	2GB	500GB	4x1GBe Ethernet, nonaccelerated
TE-810	Intel Pentium G6950	1.2 GHz	2GB	500GB	4x1GBe Ethernet, nonaccelerated
TE-820	Intel Pentium G6950	1.6 GHz	2GB	500GB	4x1GBe Ethernet, nonaccelerated
TR-1400	Intel Xeon X3450	1.6 GHz	8GB	1TB	4x1GBe Ethernet, nonaccelerated
TE-1410	Intel Xeon X3450	1.6 GHz	8GB	250GB/300GB	4x1GBe Ethernet, nonaccelerated
TE-1420	Intel Xeon X3450	2.4 GHz	8GB	250GB/300GB	4x1GBe Ethernet, nonaccelerated
PT-1400	Intel Xeon X3450	2.4 GHz	8GB	250GB	4x1GBe Ethernet, accelerated
ND-1400	Intel Xeon X3450	2.66 GHz	16GB	500GB	4x1GBe Ethernet, nonaccelerated
TR-2200	Intel Xeon E5620	2.0 GHz	12GB	1.2TB	4x1GBe Ethernet, nonaccelerated

Infoblox Model	CPU	CPU Speed	Memory	Storage[1]	Network Connectivity
TE-2210	Intel Xeon E5620	2.0 GHz	12GB	500GB/ 600GB	4x1GBe Ethernet, nonaccelerated
TE-2220	Intel Xeon E5620	2.4 GHz	12GB	500GB/ 600GB	4x1GBe Ethernet, nonaccelerated
PT-2200	Intel Xeon E5620	2.4 GHz	12GB	500GB	4x1GBe Ethernet, accelerated
ND-2200	2 x Intel Xeon E5620	2.4 GHz	24GB	1000GB	4x1GBe Ethernet, nonaccelerated
TR-4000	Intel Xeon E5-2670	2.6 GHz	24GB	1.8TB	4x1GBe Ethernet, nonaccelerated
IB-4010	Intel Xeon E5-2670	2.6 GHz	24GB	600GB	4x1GBe Ethernet, nonaccelerated
PT-4000	Intel Xeon E5-2670	2.6 GHz	24GB	600GB	4x1GBe Ethernet, accelerated
PT-4000-10G	Intel Xeon E5-2670	2.6 GHz	24GB	600GB	4x1GBe Ethernet, accelerated 10G
IB-4030	Intel Xeon E5-2670	2.6 GHz	24GB	600GB	4x1GBe Ethernet, accelerated
IB-4030-10G	Intel Xeon E5-2670	2.6 GHz	24GB	600GB	4x1GBe Ethernet, accelerated 10G
ND-4000	2 x Intel Xeon E5-2670	2.6 GHz	64GB	1200GB	4x1GBe Ethernet, nonaccelerated

1.2.1 TOE Product Type

The TOE is a network appliance which provides core network services including DNS, DHCP, IPAM, FTP, TFTP, and HTTP.

1.2.2 Required Non-TOE Hardware, Software, and Firmware

The TOE incorporates all hardware, software and firmware of the appliances listed in Table 1. Depending on the administrator defined configuration, the TOE may require the following services to be present in the environment:

- Active Directory when the TOE is configured to use an external authentication source
- NTP server when the TOE is configured to use an NTP server
- Kerberos server where GSS-TSIG or external authentication is enabled

1.3 TOE Description

This section provides context for the TOE evaluation by identifying the logical and physical scope of the TOE, as well as its evaluated configuration.

1.3.1 Physical Scope of the TOE

This section provides an overview of the Infoblox Trinzic Appliances running NIOS 7.1 Target of Evaluation (TOE). The TOE is comprised of both software and hardware. The hardware is comprised of the following: ND-800, TE-810, TE-820, TE-1410, TE-1420, PT-1400, ND-1400, TE-2210, TE- 2220, PT-2200, ND-2200, IB-4010, IB-4020, PT-4000, PT-4000-10G, IB-4030, IB-4030-10G, ND-4000. The software is comprised of the NIOS 7.1.

Common hardware characteristics of all models listed above are as follows:

- The TE and IB versions are identical in terms of hardware, but based on a software license, the CPU clock may be throttled to a lower performance level.
- The ND versions have additional memory, additional disk storage and an additional processor socket compared to the Base Appliance.
- The TR versions have additional disk storage compared to the Base Appliance.

Figure 2 below depicts the typical physical aspects of the Infoblox Trinzic Appliances.

Figure 1: Infoblox Trinzic Appliance

1.3.2 Logical Scope of the TOE

The TOE logical boundary is comprised of the following security functions:

- Security Audit
- Cryptographic Support
- Full Residual Information Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

These features are described in more detail in the subsections below. In addition, the TOE implements all SFRs of the NDPP v1.1 as necessary to satisfy testing/assurance measures prescribed therein.

Given that this Security Target conforms to the NDPP, the security claims focus on the TOE as a secure network infrastructure device and do not focus on other key functions provided by the TOE, such as Secure DNS. However, those functions can be freely used without affecting the claimed and evaluated security functions; they simply have not been evaluated to work correctly themselves.

1.3.2.1 Security Audit

The TOE generates audit records associated with use of the administrative functions. Audit records may be stored locally and sent to a syslog server. The TOE deletes the oldest records if the audit trail exceeds a defined maximum. A local time source supports reliable time stamps for the audit function. Auditable events include those requirements stated in Table 1 of the U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) ver. 1.1, dated June 8, 2012.

Note: if the TOE is configured to transmit its audit logs to an external syslog server then the communication between the TOE and the syslog server is protected by encryption.

1.3.2.2 Cryptographic Support

The TOE provides cryptography in support of Infoblox Trinzic security functionality. All algorithms have been validated against CAVP requirements (http://csrc.nist.gov/groups/STM/cavp/). See table 2 below for certificate references.

Table 2: FIPS References

Algorithm	Support Mode	CAVP Cert. #
SHS	Intel Xeon, Intel Pentium	1839
RSA/ rDSA	Intel Xeon, Intel Pentium	1085
AES	Intel Xeon, Intel Pentium	2115
HMAC	Intel Xeon, Intel Pentium	1287
RNG	Intel Xeon, Intel Pentium	1086
DRBG	Intel Xeon, Intel Pentium	835

The cryptographic services provided by the TOE are described in Table 3 below.

Table 3: TOE Provided Cryptography

Cryptographic Method	Use within the TOE
SHS	Used to provide TLS traffic integrity verification
RSA/ rDSA	Used in TLS session establishment, trusted update signature verification
AES	Used to encrypt TLS session traffic
RNG	Used in TLS session establishment
DRBG	Used in random number Generation

1.3.2.3 Full Residual Information Protection

The TOE ensures that all information flows from the TOE do not contain residual information from previous traffic. Residual data is never transmitted from the TOE. The

TOE ensures that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects by clearing the residual information before network packets are sent from the TOE.

1.3.2.4 Identification and Authentication

The TOE provides authentication services for administrative users to connect to the TOEs secure CLI administrator interface. The TOE requires Authorized Administrators to authenticate prior to being granted access to any of the management functionality. The TOE can be configured to require a minimum password length of 15 characters as well as mandatory password complexity rules. The TOE provides administrator authentication against a local user database. Password based authentication can be performed on the serial console

1.3.2.5 Security Management

The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either through a secure TLS session or via a local console connection. The TOE provides the ability to securely manage:

- All TOE administrative users;
- All identification and authentication;
- All audit functionality of the TOE;
- All TOE cryptographic functionality;
- The timestamps maintained by the TOE;
- Update to the TOE; and
- TOE configuration file storage and retrieval.

A user must have an admin account to log in to the TOE. Each admin account belongs to an admin group, which contains roles and permissions that determine the tasks a user can perform.

The TOE provides a default superuser admin group, called admin-group, with one superuser administrator, admin. The default superuser admin can log in to the TOE, using the default user name admin and password infoblox.Superuser admins are the security admins and have full access and control of all the operations of a TOE. Note that you must change the default user name and password of the default superuser admin to prevent unauthorized access
to the TOE.

Only superusers can do the following:

- Create admin accounts and groups.
- Set password parameters.
- Create the login banner.

- Set the session timeout

Limited-access admin groups provide their members with read-only or read/write access to specific resources. These admin groups can access the appliance through the GUI, API, or both. They cannot access the appliance through the console. In addition, limited-access admins are not allowed to perform the following tasks:

- Download the support bundle.
- Enable SNMP on Grid members.
- Upload files that are larger than 100 MB.

If the file size is greater than the maximum size allowed, the Upload dialog box closes and an error message is displayed in the feedback panel. The attempt to upload a file that exceeded the maximum will be logged to syslog. non-superusers only are able to upload files for file distribution and do CSV import.

1.3.2.6 Protection of the TSF

The TOE protects against interference and tampering by untrusted subjects by implementing identification, authentication, and access controls to limit configuration to Authorized Administrators. The TOE prevents reading of cryptographic keys and passwords.

1.3.2.7 TOE Access

The TOE provides administrative access via a console port (local) and HTTPS (remote). The TOE provides a password-based logon mechanism for local and remote access and enforces a defined password complexity and expiration policy. The TOE optionally supports authentication against an Active Directory server.

The TOE enforces Role Based Access Control (RBAC), session timeouts and displays an advisory banner at login.

The TOE can terminate inactive sessions after an Authorized Administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.

The TOE can also display an Authorized Administrator specified banner on the CLI management interface prior to allowing any administrative access to the TOE.

1.3.2.8 Trusted Path/Channels

The TOE initiates outbound TLS tunnels to transmit audit logs to remote syslog servers. In addition, TLS is used to secure the session between the TOE and the authentication servers.

1.4 Evaluated Configuration

In the evaluated configuration the TOE is deployed as described in the guidance documents which are delivered with the TOE. The TOE is evaluated using the following configuration settings:

- TSIG is configured for dynamic DNS updates from ISC DHCP servers and DNS clients (if applicable to the environment)
- GSS-TSIG is configured for dynamic DNS updates from Microsoft DHCP servers and DNS servers and clients (if applicable to the environment)
- bloxTools is disabled
- SSH is disabled (CLI access is performed via the local console port)
- RADIUS authentication is disabled
- TACACS+ authentication is disabled
- Secure Copy (SCP) is disabled / not used
- Grid must NOT be configured

2 Conformance Claims

This section describes the conformance claims of this Security Target.

2.1 Common Criteria Conformance Claims

The Security Target is based upon:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; Version 3.1, Revision 4, CCMB-2012-09-001;
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; Version 3.1, Revision 4, CCMB-2012-09-002;
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components; Version 3.1, Revision 4, CCMB-2012-09-003.

2.2 Protection Profile Conformance Claims

This Security Target claims the following CC conformance:

- U.S. Government Protection Profile for Security Requirements for Network Devices (NDPP) ver. 1.1, dated June 8, 2012
- Security Requirements for Network Devices Errata, ver. #3, dated 3 November 2014

2.3 Protection Profile Conformance Claim Rationale

2.3.1 TOE Appropriateness

The TOE provides all of the functionality at a level of security commensurate with that identified in the U.S. Government Protection Profile:

- U.S. Government Protection Profile for Security Requirements for Network Devices, Version 1.1
- Security Requirements for Network Devices Errata #3

2.3.2 TOE Security Problem Definition Consistency

The Assumptions, Threats, and Organization Security Policies included in the Security Target represent the Assumptions, Threats, and Organization Security Policies specified in the U.S. Government Protection Profile for Security Requirements for Network Devices Version 1.1 for which conformance is claimed verbatim. All concepts covered in the Protection Profile Security Problem Definition are included in the Security Target Statement of Security Objectives Consistency. The Security Objectives included in the Security Target represent the Security Objectives specified in the NDPPv1.1, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Objectives are included in the Security Target.

2.3.3 Statement of Security Requirements Consistency

The Security Functional Requirements included in the Security Target represent the Security Functional Requirements specified in the NDPPv1.1, for which conformance is claimed verbatim. All concepts covered in the Protection Profile's Statement of Security Requirements are included in this Security Target. Additionally, the Security Assurance Requirements included in this Security Target are identical to the Security Assurance Requirements included in section 4.3 of the NDPPv1.1.

3 Security Problem Definition Assumptions

This chapter identifies the following:

- Significant assumptions about the TOE's operational environment.
- IT related threats to the organization countered by the TOE.
- Environmental threats requiring controls to provide sufficient protection.
- Organizational security policies for the TOE as appropriate.

3.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 4: Assumptions for the TOE

Assumption Name	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

3.2 Threats

This security problem definition addresses threats posed by four categories of threat agents:

a) Persons who are not permitted to use the TOE who may attempt to use the TOE

b) Persons who are authorized to use the TOE who may attempt to use TOE functions for which they are not authorized.

c) Persons who are authorized to use the TOE who may attempt to access data in ways for which they not authorized.

d) Persons who unintentionally cause a software malfunction that may expose the TOE to unanticipated threats.

The threats and policies defined in this Security Target address the threats posed by these threat agents.

3.2.1 Threats Addressed by the TOE

This section describes the threats that are addressed by the TOE.

Table 5: Threats Addressed by the TOE

Threat	Description
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.2.2 Threats addressed by the IT Environment

There are no threats addressed by the IT Environment.

3.3 Organizational Security Policies

This section describes the Organizational Security Policies (OSPs) that apply to the TOE. OSPs are used to provide a basis for security objectives that are commonly desired by TOE Owners in this operational environment, but for which it is not practical to universally define the assets being protected or the threats to those assets.

Table 6: Organizational Security Policies for the TOE

Name	Definition
P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.

4 Security Objectives

The purpose of the security objectives is to detail the planned response to a security problem or threat. Threats can be directed against the TOE, against the security environment, or both; therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE, and
- Security objectives for the environment.

4.1 Security Objectives for the TOE

This section describes the security objectives that the TOE shall fulfill.

Table 7: Security Objectives for the TOE

Objective	Definition
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and **store** those **audit** data locally, or externally if configured.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

4.2 Security Objectives for the Operational Environment

This section describes the security objectives that must be fulfilled by the operational environment of the TOE. The following are the Protection Profile non-IT security objectives, which, in addition to those assumptions, are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8: Security Objectives for the Operational Environment

Objective	Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 Security Requirements

This section identifies the Security Functional Requirements for the TOE. The Security Functional Requirements included in this section are derived from Part 2 of the *Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, dated: September 2012* and all international interpretations.

5.1 Conventions

The CC defines operations on Security Functional Requirements: assignments, selections, assignments within selections and refinements. This document uses the following font conventions to identify the operations defined by the CC:

- Assignment: Indicated with *italicized* text;
- Refinement: Indicated with **bold** text;
- Selection: Indicated with underlined text;
- Iteration: Indicated by appending the iteration number in parenthesis, e.g., (1), (2), (3).
- Where operations were completed in the NDPP itself, the formatting used in the NDPP has been retained.

Explicitly stated SFRs are identified by having a label 'EXT' after the requirement name for TOE SFRs. Formatting conventions outside of operations and iterations matches the formatting specified within the NDPP.

5.2 TOE Security Functional Requirements

This section identifies the Security Functional Requirements for the TOE. The TOE Security Functional Requirements that appear in the following table are described in more detail in the following subsections.

Table 9: Security Functional Requirements

Class Name	Component Identification	Component Name
FAU: Security audit	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User Identity Association
	FAU_STG_EXT.1	External Audit Trail Storage
FCS: Cryptographic support	FCS_CKM.1	Cryptographic Key Generation (for asymmetric keys)
	FCS_CKM_EXT.4	Cryptographic Key Zeroization
	FCS_COP.1(1)	Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2)	Cryptographic Operation (for cryptographic signature)

Class Name	Component Identification	Component Name
	FCS_COP.1(3)	Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4)	Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1	Extended: HTTPS
	FCS_RBG_EXT.1	Extended: Cryptographic Operation (Random Bit Generation)
	FCS_TLS_EXT.1	TLS
FDP: User Data Protection	FDP_RIP.2	Full Residual Information Protection
FIA: Identification and authentication	FIA_PMG_EXT.1	Password Management
	FIA_UIA_EXT.1	User Identification and Authentication
	FIA_UAU_EXT.2	Password-based Authentication Mechanism
	FIA_UAU.7	Protected Authentication Feedback
FMT: Security Management	FMT_MTD.1	Management of TSF Data (for general TSF data)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.2	Restrictions on Security Roles
FPT: Protection of the TSF	FPT_SKP_EXT.1	Extended: Protection of Secret Key Parameters
	FPT_APW_EXT.1	Extended: Protection of Administrator Passwords
	FPT_STM.1	Reliable Time Stamps
	FPT_TUD_EXT.1	Extended: Trusted Update
	FPT_TST_EXT.1	TSF Testing
FTA: TOE Access	FTA_SSL_EXT.1	TSF-initiated Session Locking
	FTA_SSL.3	TSF-initiated Termination
	FTA_SSL.4	User-initiated Termination
	FTA_TAB.1	Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1	Inter-TSF Trusted Channel
	FTP_TRP.1	Trusted Path

5.2.1 Security Audit (FAU)

5.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shut-down of the audit functions;

b) All auditable events for the not specified level of audit; and

c) All administrative actions;

d) [Specifically defined auditable events listed in Table 10].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of Table 10].

Table 10: Auditable Events

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	Start of audit Shutdown of audit	None.
FAU_GEN.2	None.	None.
FAU_STG_EXT.1	None.	None.
FCS_CKM.1	None.	None.
FCS_CKM_EXT.4	None.	None.
FCS_COP.1(1)	None.	None.
FCS_COP.1(2)	None.	None.
FCS_COP.1(3)	None.	None.
FCS_COP.1(4)	None.	None.
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session. Establishment/Termination of a HTTPS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_RBG_EXT.1	None.	None.
FCS_TLS_EXT.1	Failure to establish a TLS Session. Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both success and failures.
FDP_RIP.2	None.	None.

Requirement	Auditable Events	Additional Audit Record Contents
FIA_PMG_EXT.1	None.	None.
FIA_UIA_EXT.1	All use of the identification and authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU_EXT.2	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	None.
FMT_MTD.1	None.	None.
FMT_SMF.1	Changes to audit function	None.
FMT_SMR.2	None.	None.
FPT_SKP_EXT.1	None.	None.
FPT_APW_EXT.1	None.	None.
FPT_ITT.1	None.	None.
FPT_STM.1	Changes to the time	The old and new values for the time. Origin of the attempt (e.g., IP address).
FPT_TUD_EXT.1	Initiation of update	None.
FPT_TST_EXT.1	None.	None.
FTA_TAB.1	None.	None.
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt
FTP_TRP.1	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

5.2.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 FAU_STG_EXT.1 External Audit Trail Storage

FAU_STG_EXT.1.1 The TSF shall be able to [selection: transmit the generated audit data to an external IT entity] using a trusted channel implementing the [selection: TLS] protocol.

5.2.2 Cryptographic Support (FCS)

5.2.2.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

FCS_CKM.1.1

Refinement: The TSF shall generate **asymmetric** cryptographic keys **used for key establishment** in accordance with [selection: NIST Special Publication 800-56B, “Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography” for RSA-based key establishment schemes] and specified cryptographic key sizes *equivalent to, or greater than, a symmetric key strength of 112 bits*.

5.2.2.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

FCS_CKM_EXT.4.1

The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.2.2.3 FCS_COP.1 (1) Cryptographic Operation (for data encryption/decryption)

FCS_COP.1.1 (1)

Refinement: The TSF shall perform [*encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES operating in* [**selection: CBC**] and cryptographic key sizes 128-bits and 256-bits that meets the following:

- **FIPS PUB 197, “Advanced Encryption Standard (AES)”**
- **[selection: NIST SP 800-38A, NIST SP 800-38D]**

5.2.2.4 FCS_COP.1 (2) Cryptographic Operation (for cryptographic signature)

FCS_COP.1.1 (2)

Refinement: The TSF shall perform cryptographic signature services in accordance with a [selection: **RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater.]** that meets the following **FIPS PUB 186-3, “Digital Signature Standard”**.

5.2.2.5 FCS_COP.1 (3) Cryptographic Operation (for cryptographic hashing)

FCS_COP.1.1 (3) **Refinement**: The TSF shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm **[selection: SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [selection: 160, 256, 384, 512] bits** that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

5.2.2.6 FCS_COP.1 (4) Cryptographic Operation (for keyed-hash message authentication)

FCS_COP.1.1 (4) **Refinement:** The TSF shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm HMAC-**[selection: SHA-1, SHA-256, SHA-384, SHA-512], key size [assignment: *160, 256, 384, 512 bits*]**, **and message digest sizes [selection: 160, 256, 384, 512] bits** that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."*

5.2.2.7 FCS_HTTPS_EXT.1 Explicit: HTTPS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

5.2.2.8 FCS_RBG__EXT.1 Extended: Cryptographic Operation (Random Bit Generation)

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: HMAC_DRBG (any)]; seeded by an entropy source that accumulated entropy from [selection, one or both of: a TSF-hardware-based noise source].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [selection: 256 bits] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

5.2.2.9 FCS_TLS_EXT.1 Explicit TLS

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[selection:

TLS_RSA_WITH_AES_256_CBC_SHA

TLS_DHE_RSA_WITH_AES_128_CBC_SHA

TLS_DHE_RSA_WITH_AES_256_CBC_SHA].

5.2.3 User Data Protection (FDP)

5.2.3.1 FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: allocation of the resource to] all objects.

5.2.4 Identification and Authentication (FIA)

5.2.4.1 FIA_PMG_EXT.1 Password Management

FIA_PMG_EXT.1.1 The TSF shall provide the following password management capabilities for administrative passwords:

1. Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and the following special characters: [selection: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)];

2. Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;

5.2.4.2 FIA_UIA_EXT.1 User Identification and Authentication

FIA_UIA_EXT.1.1 The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- Display the warning banner in accordance with FTA_TAB.1;
- [selection: no other actions].

FIA_UIA_EXT.1.2 The TSF shall require each administrative user to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of that administrative user.

5.2.4.3 FIA_UAU_EXT.2 Extended: Password-based Authentication Mechanism

FIA_UAU_EXT.2.1 The TSF shall provide a local password-based authentication mechanism, [selection: [assignment:

Authentication using Active Directory Server]] to perform administrative user authentication.

5.2.4.4 FIA_UAU.7 Protected Authentication Feedback

FIA_UAU.7.1 The TSF shall provide only *obscured feedback* to the administrative user while the authentication is in progress at the local console.

5.2.5 Security Management (FMT)

5.2.5.1 FMT_MTD.1 Management of TSF Data (for general TSF data)

FMT_MTD.1.1 The TSF shall restrict the ability to *manage* the *TSF data* to the *Security Administrators*.

5.2.5.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- *Ability to administer the TOE locally and remotely;*
- *Ability to update the TOE, and to verify the updates using [selection: digital signature] capability prior to installing those updates;*
- *[selection: Functions listed in Table 14.]*

5.2.5.3 FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles:

- **Authorized Administrator.**

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions

- **Authorized Administrator role shall be able to administer the TOE locally;**
- **Authorized Administrator role shall be able to administer the TOE remotely;**

are satisfied.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 FPT_APW_EXT.1 Protection of Administrator Passwords

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

5.2.6.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

5.2.6.3 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2.6.4 FPT_TUD_EXT.1 Extended: Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide security administrators the ability to query the current version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide security administrators the ability to initiate updates to TOE firmware/software.

FPT_TUD_EXT.1.3 The TSF shall provide a means to verify firmware/software updates to the TOE using a [selection: digital signature mechanism] prior to installing those updates.

5.2.6.5 FPT_TST_EXT.1 TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

5.2.7 TOE Access (FTA)

5.2.7.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection: terminate the session] after a Security Administrator-specified time period of inactivity.

5.2.7.2 FTA_SSL.3 TSF-initiated Termination

FTA_SSL.3.1 **Refinement**: The TSF shall terminate **a remote interactive** session after a [*Security Administrator-configurable time interval of session inactivity*].

5.2.7.3 FTA_SSL.4 User-initiated Termination

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator’s own interactive session.

5.2.7.4 FTA_TAB.1 TOE Access Banner

FTA_TAB.1.1 **Refinement:** Before establishing **an administrative user** session the TSF shall display **a Security Administrator-specified** advisory **notice and consent** warning message regarding use of the TOE.

5.2.8 Trusted Path/Channels (FTP)

5.2.8.1 FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 **Refinement:** The TSF shall **use [selection: TLS]** to provide a **trusted** communication channel between itself and **authorized IT entities supporting the following**

capabilities: audit server, [selection: *assignment: authentication of administrator to Active Directory*]] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data **from disclosure and detection of modification of the channel data**.

FTP_ITC.1.2 The TSF shall permit *the TSF*, ***or the authorized IT entities*** to initiate communication via the trusted channel.

FTP_ ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment: *authentication of administrator to Active Directory, sending of audit events*.]

5.2.8.2 FTP_TRP.1 Trusted Path

FTP_TRP.1.1 **Refinement:** The TSF shall **use [selection: TLS/HTTPS]** provide **a trusted** communication path between itself and **remote administrators** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from *disclosure and detection of modification of the communicated data*.

FTP_TRP.1.2 **Refinement:** The TSF shall permit **remote administrators** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for *initial administrator authentication and all remote administration actions*.

5.3 Rationale for Extended Security Functional Requirements

The Security Functional Requirements (SFRs) in this Security Target represent the SFRs identified in the NDPPv1.1. As such, the NDPP SFR dependency rationale is deemed acceptable since the PP itself has been validated.

5.4 Security Assurance Requirements

5.4.1 SAR Requirements

The TOE assurance requirements for this ST are taken directly from the NDPP which are derived from Common Criteria Version 3.1, Revision 4. The assurance requirements are summarized in the table below.

Table 11: Assurance Components

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance

Assurance Class	Assurance Components	Assurance Components Description
	AGD_PRE.1	Preparative User Guidance
Tests	ATE_IND.1	Independent testing - Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Analysis
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage

5.4.2 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs) in this Security Target represent the SARs identified in the NDPPv1.1. As such, the NDPP SAR rationale is deemed acceptable since the PP itself has been validated.

5.5 Assurance Measures

The TOE satisfies the identified assurance requirements. This section identifies the Assurance Measures applied by Infoblox to satisfy the assurance requirements. The table below lists the details.

Table 12: Assurance Measures

Component	How requirement will be met
ADV_FSP.1	The functional specification describes the external interfaces of the TOE; such as the means for a user to invoke a service and the corresponding response of those services. The description includes the interface(s) that enforces a security functional requirement, the interface(s) that supports the enforcement of a security functional requirement, and the interface(s) that does not enforce any security functional requirements. The interfaces are described in terms of their purpose (general goal of the interface), method of use (how the interface is to be used), parameters (explicit inputs to and outputs from an interface that control the behavior of that interface), parameter descriptions (tells what the parameter is in some meaningful way), and error messages (identifies the condition that generated it, what the message is, and the meaning of any error codes). The development evidence also contains a tracing of the interfaces to the SFRs described in this ST.
AGD_OPE.1	The Administrative Guide provides the descriptions of the processes and procedures of how the administrative users of the TOE can securely administer the TOE using the interfaces that provide the features and functions detailed in the guidance.
AGD_PRE.1	The Installation Guide describes the installation, generation and startup procedures so that the users of the TOE can put the components of the TOE in the evaluated configuration.
ATE_IND.1	Infoblox will provide the TOE for testing
AVA_VAN.1	Infoblox will provide the TOE for testing

Component	How requirement will be met
ALC_CMC.1	The Configuration Management (CM) document(s) describes how the consumer (end-user) of the TOE can identify the evaluated TOE (Target of Evaluation). The CM document(s), identifies the configuration items, how those configuration items are uniquely identified, and the adequacy of the procedures that are used to control and track changes that are made to the TOE. This includes details on what changes are tracked, how potential changes are incorporated, and the degree to which automation is used to reduce the scope for error.
ALC_CMS.1	

6 TOE Summary Specification

6.1 TOE Security Functional Requirement Measures

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

- Security Audit
- Cryptographic Support
- Full Residual Information Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Trusted Path/Channels

6.1.1 Security Audit

Related SFRs:	FAU_GEN.1, FAU_GEN.2, FAU_STG._EXT.1

The TOE generates an audit record of the following auditable events: Start-up and shutdown of the audit functions; All auditable events for the basic level of audit; All administrative actions; and specifically defined auditable events listed in Table 10.

The TOE records within each audit record the following information: Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and for each audit event type, based on the auditable event definitions of the functional components, information specified in column three of Table 10.

For audit events resulting from actions of identified users, the TOE associates each auditable event with the identity of the user that caused the event.

The audit log is stored locally by default, and the TOE protects the stored audit records in the audit trail from unauthorized deletion and prevents unauthorized modifications to the stored audit records in the audit trail.

Specifically, the security related audit logs are kept in two separate log files:

- Audit Log – Maintains audit records for all admin management functionality;
- syslog – Maintains audit records of DNS and network traffic;

The Audit Log is accessible only to the superuser. The syslog is accessible to users with superuser admin, DNS Administrator, or DHCP Administrator privileges. The TOE deletes the oldest audit records if the audit trail exceeds 1,000,000,000 bytes.

The local time source supports the reliable time stamp for audit function.

The Audit Log and syslog records are transmitted to an external Syslog Server. Audit records are transmitted through a secure TLS connection immediately after they are generated. If the connection to the external Syslog server fails the message will be audited locally on the TOE and there will be an additional audit message regarding the failure.

6.1.2 Cryptographic Support

Related SFRs: FCS_CKM.1, FCS_CKM_EXT.4, FCS_COP.1(1), FCS_COP.1(2), FCS_COP.1(3), FCS_COP.1(4), FCS_RGB.1

The TOE uses the NIOS Cryptographic Library version 1.0 (Firmware) to implement all cryptographic functions.In support of secure cryptographic protocols, the TOE supports key establishment schemes, as specified in SP NIST 800-56B without extensions. All shall not and should not are not implemented and all shall and should operations are implemented.

The TOE zeroizes all plaintext secret and private cryptographic keys and Cryptographic Critical Security Parameters (CSPs) when no longer required. While the administrator could directly read RAM or persistent memory to view CSPs, they are trusted not to do so.

The TOE performs encryption and decryption in accordance with cryptographic algorithm AES operating in CBC mode and cryptographic key sizes 128-bits, 256-bits, and 192-bits. FIPS PUB 197 and NIST SP 800-38B are met for AES implementation. AES is implemented in the following protocols: TLS. The relevant CAVP certificate numbers are listed in Table 2, Section 1.3.2.2.

The TOE performs cryptographic signature services in accordance with RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater. It meets the requirements of RSA Digital Signature in FIPS PUB 186-3.

The TOE performs cryptographic hashing services in accordance with SHA-1, SHA-256, SHA-384, and SHA-512 and message digest sizes 160, 256, 384, and 512 bits. FIPS Pub 180-3 is met for SHA implementation.

The TOE performs keyed-hash message authentication in accordance with HMAC-SHA-1, SHA-256, SHA-384, SHA-512, key size 128, 256 and 512 bits, and message digest sizes 160, 256, 384, 512 bits. FIPS Pub 198 and FIPS Pub 180-2 are met for HMAC implementation.

NIOS random numbers are generated with a NIST SP 800-90A HMAC SHA-1 Deterministic Random Bit Generator (DRBG). The entropy source is a hardware based noise generator.

The table below identifies all secret and private keys and CSPs used to generate keys, the related zeroization procedures and whether any interface is available to view the plaintext key.

Table 13: Keys, zeroization and interfaces

Key/CSP	Location	Zeroization procedure	Interface
HTTPS server private key: 2048 bit RSA	Encrypted database file	Overwritten when no longer in use; three times with a random pattern, and once with zeroes.	Not readable via any normal interface.
Static symmetric key for decrypting software updates (AES-256-CBC)	Compiled into a library binary.	None. Key remains static.	Not readable by any normal interface.
Static symmetric key for encrypting/decrypting database backups (AES-128-CBC)	Compiled into a library binary.	None. Key remains static.	Not readable by any normal interface.
DNS GSS-TSIG shared keys	Stored in the database and in files. Encrypted in database backups.	None. Key remains static.	Not readable by any normal interface.
Administration session cookie HMAC key: HMAC-SHA1	File	Overwritten when no longer in use; three times with a random pattern, and once with zeroes.	Not readable by any normal interface.
TLS session keys	Stored in memory	Overwritten with zeroes when no longer in use	Not readable by any normal interface.
RBG state seed	Process memory	The generator state is overwritten with zeroes when the generator process exits, at system shutdown.	Not readable by any normal interface.

6.1.3 Full Residual Information Protection

Related SFRs:	FDP_RIP.2

The TOE ensures that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects by clearing the residual information before network packets are sent from the TOE.

Specifically, all network traffic goes through socket buffers allocated and managed by the kernel. The routines for allocation are centralized and all appropriate zeroing and initialization is handled by routines in the sk_buff routines.

The Kernel guarantees the clearing of the memory from one process invocation to the next and thereby makes certain that there can be no leaking of information between connections managed by different processes.

The user level code, i.e. programs listed below, also implements mechanisms to ensure that residual information shall not be leaked:

- named (DNS):

  TCP replies use buffers managed by a Bind specific package that handles the initialization (zeroing) of all buffers.

  UDP replies use buffers that are re-used without explicit clearing, but the code is specifically written to always write in new data for all parts of the buffer that is actually sent (i.e. the buffer is overwritten).

  Named, as part of its base functionality, uses internal caches to store information which is used in multiple different replies (to different clients), the information here is however not private to any client and the caches does not re-use any actual reply packages or query information.

- dhcpd (DHCP):

  The DHCP server only sends UDP messages to clients and uses the same technique as described above in named (DNS) (and the same underlying library).

  httpd (Apache, web server):

  Httpd has been written to use buffer and memory management from the Apache Portable Runtime Library (APR). The APR overwrites the buffer to prevent it from re-use.

- syslog-ng (syslog):

  The syslog daemon can be used to forward log messages. All buffers used by syslog-ng for message sent over the network are handled by the GString package from glib (GNOME C lib), this package handles strings with lengths and is used in such a way that all possible previous data is overwritten with new data before anything is sent.

- ntpd (NTP):

  Ntpd sends packets by filling in structures representing the protocol on the wire, i.e. the data buffer is overwritten.

  Note that, the requirement of reliable time stamp is not implemented by NTP. Instead, it is supported by local time source.

6.1.4 Identification and Authentication

Related SFRs: FIA_PMG_EXT.1, FIA_UIA_EXT.1, FIA_UAU_EXT.2, FIA_UAU.7, FPT_APW_EXT.1

The TOE provides the administrator access to the TOE via console port (locally) and HTTPS (remotely). The TOE provides a password-based logon mechanism for authorized access to the TOE locally or remotely. The authentication policy can be configured to specify whether authentication uses a local store or through invoking authentication services from a remote Active Directory server. Local password representations are stored in SHA-1 hash format.

The TOE allows no services on behalf of the user to be performed before the user is identified and authenticated, and requires each user to be successfully identified and authenticated before allowing any other actions on behalf of that user.

The TOE enforces the following password policy for administrative passwords:

- Passwords shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters (that include: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “)”);
- Minimum password length shall settable by the Security Administrator, and support passwords of 15 characters or greater;
- Passwords composition rules specifying the types and number of required characters that comprise the password shall be settable by the Security Administrator.
- Passwords shall have a maximum lifetime, configurable by the Security Administrator.
- New passwords must contain a minimum of 4 character changes from the previous password.

The TOE implements that users with expired passwords are required to create a new password after correctly entering the expired password. The TOE re-authenticates the user when the user changes their password, or following session locking.

The TSF provides only obscured feedback to the user while the authentication is in progress at both the local console and remote HTTPS access.

For remote access, after the user is authenticated, the TOE checks for the user roles before the dashboard are displayed. The available options on the dashboard are determined by the user role.

For local console access, only users with the superuser admin privilege may use this interface. Once authenticated, the superuser admin is provided an Infoblox console prompt.

6.1.5 Security Management

Related SFRs:	FMT_SMF.1, FMT_MTD.1, FMT_SMR.2

A user must have an admin account to log in to the TOE. Each admin account belongs to an admin group, which contains roles and permissions that determine the tasks a user can perform.

The TOE provides two interfaces to manage its security functions and data, the GUI interfaces access remotely through HTTPS and the local console. All users accessing the

TOE must be identified and authenticated. Access to security management functions is restricted to specific user roles.

Administrative users can be assigned different access privileges when the user is created. The available privileges include:

- superuser admin
- DNS Admin
- DHCP Admin
- File Distributor Admin

The superuser admin privilege gives full access to the TOE and includes the other three privileges. The TOE construct of Security Administrator equates to a TOE administrative user with the superuser admin privilege. The TOE construct of Authorized Administrator equates to a TOE administrative user with any of the TOE privileges.

The TSF is capable of performing the following management functions:

Table 14: Management Functions

Management Function	User privileges			
	superuser Admin	DNS Admin	DHCP Admin	File Distributor Admin
Manage authentication policy	Modify			
Manage password policy	Modify			
Manage user creation/modification	Modify			
Manage the TOE banner	Modify	Enable	Enable	
Manage TOE updates	Modify			
Manage TOE Session Inactivity	Modify			
Manage audit configuration for external audit	Modify			
Manage TOE system time	Modify	Read	Read	Read
Manage own password	Modify	Modify	Modify	Modify

Management functions description

Manage password policy – Gives the administrator the ability to define the global policy for password metrics.

Manage user creation/modification – Gives the administrator the ability to create, modify, and delete user accounts and user groups.

Manage authentication policy – Gives the administrator the ability to define method of authentication whether local or remote and identifying the remote authentication server. This is a group policy setting for all users within the specified user group.

Manage the TOE banner – Gives the administrator the ability to configure the warning message that users see at the login display.

Manage TOE Session Inactivity – Gives the administrator the ability to define interactive session timers.

Manage audit configuration for external audit – Gives the administrator the ability to configure the location of the external syslog server and which logs are to be transmitted.

Manage TOE system time – Gives the administrator the ability to change the local system time and configure the use of a NTP server.

Manage own password – Gives the administrator the ability to change their own passwords.

6.1.6 Protection of the TOE

Related SFRs: FPT_SKP_EXT.1, FPT_APW_EXT.1, FPT_STM.1, FPT_TUD_EXT.1, FPT_TST_EXT.1

The TOE includes CLI command features that can be used to initially configure the TOE to encrypt all locally defined user passwords. The TOE ensures that plaintext user passwords will not be disclosed even to administrators.

The TOE stores all private keys in a secure directory that is not readily accessible to administrators; hence no interface access. Additionally, all passwords, pre-shared and symmetric keys are stored in encrypted form to prevent access.

The TOE provides a source of date and time information used in audit event timestamps. The clock function is reliant on the system clock provided by the underlying hardware. The TOE can optionally be set to receive clock updates from an NTP server. This date and time is used as the time stamp that is applied to TOE generated audit records and used to track inactivity of administrative sessions. This system clock is also used for cryptographic functions.

Authorized Administrator can query the software version running on the TOE, and can initiate updates to (replacements of) software images. When software updates are made available by Infoblox, an administrator can obtain, verify the integrity of, and install those updates. The updates can be downloaded from the support.infoblox.com. The TOE image files are digitally signed so their integrity can be verified during the boot process, and an image that fails an integrity check will not be loaded. The digital certificates used by the update verification mechanism are contained on the TOE. Specifically, Infoblox generates RSA digital signature for TOE updates to ensure that the update can be trusted. The TOE verifies the digital signature associated with the TOE update. The certificate used for validation is stored in a protected file on the appliance. Detailed instructions for how to do this verification are provided in the administrator guidance for this evaluation.

The CLI shows the version of the TOE on login and provides a command to show the version of TOE and serial number of unit. Upgrade functionality allows for updating the TOE software after validating a digital signature on the software.

The TOE implements self-test, during initial startup, to determine whether the TOE is operating correctly. The self-test includes:

- Memory test using the MemBIST test from the Intel memory reference code (MRC); at the end of the test faulty isolated memory are disabled;
- Crytographic libraries test where library content is compared to a stored checksum;
- Crypto algorithms known answer tests are executed for all algorithms;
- Random number generation test, which continuously test the seed entropy using a Repetition Count test and an Adaptive Proportion test.

If any of these tests fail, the system startup will be aborted and an error message will be displayed on the serial console and on the LCD. Otherwise, the login prompt will be displayed showing that the system is operating correctly. The TOE will log to the syslog when the test runs on power-up, either successful or failure.

6.1.7 TOE Access

Related SFRs:	FTA_SSL_EXT.1, FTA_SSL.3, FTA_SSL.4; FTA_TAB.1

For local interactive sessions, the TOE terminates the session after an administrator configured time period of inactivity. The TOE also terminates a remote interactive session after an administrator configured time interval of session inactivity. The TOE allows user termination of their own interactive sessions.

Before establishing a user/administrator session, the TOE displays an administrator configured advisory banner and consent warning message regarding unauthorized use of the TOE.

6.1.8 Trusted Path/Channels

Related SFRs:	FTP_ITC.1, FPT_TRP.1, FCS_HTTPS_EXT.1, FCS_TLS_EXT.1

The TOE communicates with other network devices, as well as administrators, over the network. The critical communication paths and their related protection mechanisms are as follows:

- **Remote Administration -** Remote administrators configure the TOE via a web based GUI that is protected using TLS/HTTPS.
- **Syslog Server** – All communication with the syslog server is protected with TLS
- **Active Directory Server** - All communication with the active directory server is protected with TLS

The following sections provide further detail on each of the secure communication protocols identified above and the associated supporting cryptography.

TLS/HTTPS

The TOE implements TLS 1.0 (RFC 2246), supporting the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA,
- TLS_RSA_WITH_AES_256_CBC_SHA,
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA, and
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA.

The TOE implements the HTTPS protocol that complies with RFC 2818 using TLS 1.0. This implementation uses Apache 2.2 (mod_ssl) and OpenSSL 1.0.0k)(with FIPS extensions) on port 443. The TLS configuration is not modifiable once the TOE is installed and operational. For remote administration, client authentication is not supported.

The TOE (as server) uses a 2048 bit RSA key. The server certificate may be self-signed or signed by an external CA using a CSR generated by the TOE. The certificate is used by the TOE to authenticate itself for incoming TLS connections. The certificate (and authentication) is used by administrative clients (GUI, API) that connect to the TOE. Client TLS authentication is not used. Session resumption is supported.

The TOE (as client) connects to secure Syslog and active directory servers. The TOE validates server certificates with validation certificates (CAs) installed by the administrator.

7 Glossary

For the purposes of this document, the following terms and definitions apply.

Table 15: Acronyms

Acronym	Definition
A.	assumption (when used in hierarchical naming)
CC	Common Criteria
EAL	evaluation assurance level
IT	information technology
O.	security objective (of the TOE) (when used in hierarchical naming)
OE.	security objective (of the operational environment) (when used in hierarchical naming)
OSP	organizational security policy
P.	organizational security policy (when used in hierarchical naming)
PP	protection profile
SFP	security function policy
SFR	security functional requirement
ST	security target
T.	threat (when used in hierarchical naming)
TOE	Target of Evaluation
TSF	TOE security functionality
TSP	TOE security policy

8 References

1. Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4 - Part 1: Introduction and General Model

2. Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4 – Part 2: Security Functional Requirements

3. Common Criteria for Information Technology Security Evaluation Version 3.1 Release 4 – Security Assurance Requirements

4. Common Methodology for Information Technology Security Evaluation Version 3.1 Release 4 - Evaluation Methodology

5. Protection Profile for Network Devices, Version 1.1, dated June 8, 2012

6. Security Requirements for Network Devices Errata #3, dated November 3, 2014