Intrusion Detection in the HP Enterprise LaserJet, Officejet, and PageWide SFP and MFP FutureSmart Firmware Security Target

Version:	**2.3**
Status:	**Final**
Last Update:	**2019-04-15**

Trademarks

The following term is a trademark of atsec information security corporation in the United States, other countries, or both.

- atsec®

The following terms are trademarks of Hewlett-Packard Development Company, L.P. in the United States, other countries, or both.

- HP®
- LaserJet®
- Officejet®
- PageWide®

The following term is a trademark of Massachusetts Institute of Technology (MIT) in the United States, other countries, or both.

- Kerberos™

The following terms are trademarks of Microsoft Corporation in the United States, other countries, or both.

- Microsoft®
- SharePoint®
- Windows®

The following terms are trademarks of INSIDE Secure in the United States, other countries, or both.

- INSIDE Secure®
- QuickSec®

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
2.3	2019-04-15	Scott Chapman	Initial version.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	Intrusion Detection in the HP Enterprise LaserJet, Officejet, and PageWide SFP and MFP FutureSmart Firmware Security Target
Version:	2.3
Status:	Final
Date:	2019-04-15
Sponsor:	HP Inc.
Developer:	HP Inc.
Certification Body:	CSEC
Certification ID:	CSEC 2016006
Keywords:	HP Inc., HP, Color LaserJet, LaserJet, Officejet, PageWide, 556, 586, M506, M525, M527, M553, M575, M577, M605, M606, M630, M651, M680, M725, M830, M855, M880, X555, X585, hardcopy device, HCD, single-function printer, SFP, multifunction printer, MFP, intrusion detection

1.2 TOE Identification

The TOE is the HP Enterprise LaserJet, Officejet, and PageWide single-function printer (SFP) and multifunction printer (MFP) FutureSmart firmware.

1.3 TOE Type

The TOE type is the internal firmware providing intrusion detection and other security functionality for both SFPs and MFPs.

1.4 TOE Overview

The target of evaluation (TOE) resides on models that are enterprise network SFPs and MFPs, collectively called hardcopy devices (HCDs).

The TOE contains intrusion detection functionality as well as the typical HCD functions for copying, printing, faxing, scanning and storing of documents. (Not all HCD models provide the ability to copy, fax, and scan.) Each HCD is a self-contained unit that includes processors, memory, networking, a storage drive, and a print engine. The operating system, web servers, and Control Panel applications (i.e., applications that run internally on the HCD) reside within the firmware of the HCD.

The TOE is the contents of the firmware with the exception of the QuickSec cryptographic library (used by the Internet Protocol Security (IPsec)), which is part of the Operational Environment.

The HCD models for which the firmware is evaluated are listed in Table 1 along with the evaluated firmware version numbers for each model.

Product Family	HCD Model	Type	TOE Firmware Version
HP PageWide Enterprise Color Printer 556 Series	Printer 556dn, Printer 556xh	SFP	System Firmware version: 2405268_022711 Jetdirect Inside version: JSI24050246

Product Family	HCD Model	Type	TOE Firmware Version
HP PageWide Enterprise Color MFP 586 Series	MFP 586dn, MFP 586f, Flow MFP 586z	MFP	System Firmware version: 2405268_022716 Jetdirect Inside version: JSI24050246
HP LaserJet Enterprise Printer M506 Series	Printer M506x	SFP	System Firmware version: 2405268_022717 Jetdirect Inside version: JSI24050246
HP LaserJet Enterprise 500 MFP M525 Series	MFP M525dn, MFP M525f, Flow MFP M525c	MFP	System Firmware version: 2405268_022702 Jetdirect Inside version: JDI24050229
HP LaserJet Enterprise MFP M527 Series	MFP M527dn, MFP M527f, Flow MFP M527c, Flow MFP M527z	MFP	System Firmware version: 2405268_022698 Jetdirect Inside version: JSI24050246
HP Color LaserJet Enterprise Printer M553 Series	Printer M553x	SFP	System Firmware version: 2405268_022726 Jetdirect Inside version: JSI24050246
HP LaserJet Enterprise 500 color MFP M575 Series	MFP M575dn, MFP M575f, Flow MFP M575c	MFP	System Firmware version: 2405268_022704 Jetdirect Inside version: JDI24050229
HP Color LaserJet Enterprise MFP M577 Series	MFP M577dn, MFP M577f, Flow MFP M577c, Flow MFP M577z	MFP	System Firmware version: 2405268_022696 Jetdirect Inside version: JSI24050246
HP LaserJet Enterprise Printer M605 Series	Printer M605x	SFP	System Firmware version: 2405268_022718 Jetdirect Inside version: JSI24050246
HP LaserJet Enterprise Printer M606 Series	Printer M606x	SFP	System Firmware version: 2405268_022718 Jetdirect Inside version: JSI24050246
HP LaserJet Enterprise MFP M630 Series	MFP M630dn, MFP M630f, MFP M630h, Flow MFP M630z	MFP	System Firmware version: 2405268_022701 Jetdirect Inside version: JDI24050229
HP Color LaserJet Enterprise Printer M651 Series	Printer M651n, Printer M651dn, Printer M651xh	SFP	System Firmware version: 2405268_022703 Jetdirect Inside version: JDI24050229
HP Color LaserJet Enterprise MFP M680 Series	MFP M680dn, MFP M680f, Flow MFP M680z	MFP	System Firmware version: 2405268_022738 Jetdirect Inside version: JDI24050229
HP LaserJet Enterprise MFP M725 Series	MFP M725dn, MFP M725f, MFP M725z, MFP M725z+	MFP	System Firmware version: 2405268_022740 Jetdirect Inside version: JDI24050229
HP LaserJet Enterprise flow MFP M830 Series	Flow MFP M830z, Flow MFP M830z+	MFP	System Firmware version: 2405268_022741 Jetdirect Inside version: JDI24050229

Product Family	HCD Model	Type	TOE Firmware Version
HP Color LaserJet Enterprise Printer M855 Series	Printer M855dn, Printer M855xh, Printer M855x+	SFP	System Firmware version: 2405268_022724 Jetdirect Inside version: JDI24050229
HP Color LaserJet Enterprise flow MFP M880 Series	Flow MFP M880z, Flow MFP M880z+	MFP	System Firmware version: 2405268_022739 Jetdirect Inside version: JDI24050229
HP Officejet Enterprise Color Printer X555 Series	Printer X555dn, Printer X555xh	SFP	System Firmware version: 2405268_022721 Jetdirect Inside version: JDI24050229
HP Officejet Enterprise Color MFP X585 Series	MFP X585dn, MFP X585f, Flow MFP X585z	MFP	System Firmware version: 2405268_022705 Jetdirect Inside version: JDI24050229

Table 1: TOE Reference

Each TOE model provides the following security features.

- Auditing
- Cryptography
- Identification and authentication
- Protection of the TOE Security Functionality (TSF) (intrusion detection, timestamps)
- TOE access protection (inactivity timeout)
- Trusted channel communication and certificate management
- Security management

1.4.1 Required and optional non-TOE hardware, software, and firmware

The following *required* firmware component is considered part of the Operational Environment.

- QuickSec cryptographic library module (included in the firmware)

The hardware portion of the HCD models is considered part of the Operational Environment. The TOE is evaluated on all of the HCD models defined in Table 1 and *requires* one of these models in order to run in the evaluated configuration.

The following *required* components are part of the Operational Environment.

- Domain Name System (DNS) server
- Syslog server
- Windows Internet Name Service (WINS) server
- One administrative client computer network connected to the TOE in the role of an Administrative Computer
- Web browser installed on the Administrative Computer

The following *optional* components are part of the Operational Environment.

- HP Print Drivers, including the HP Universal Print Driver, for client computers (for submitting print job requests from client computers)
- Windows domain controller/Kerberos server

- Lightweight Directory Access Protocol (LDAP) server
- Client computers network connected to the TOE in a non-administrative computer role
- Remote file systems:
  - Server Message Block (SMB)
  - FTP
- Microsoft SharePoint server (useful with *flow* models only)
- Simple Mail Transfer Protocol (SMTP) gateway (a.k.a. email server)

Figure 1 shows how HCDs are deployed in a typical customer environment.

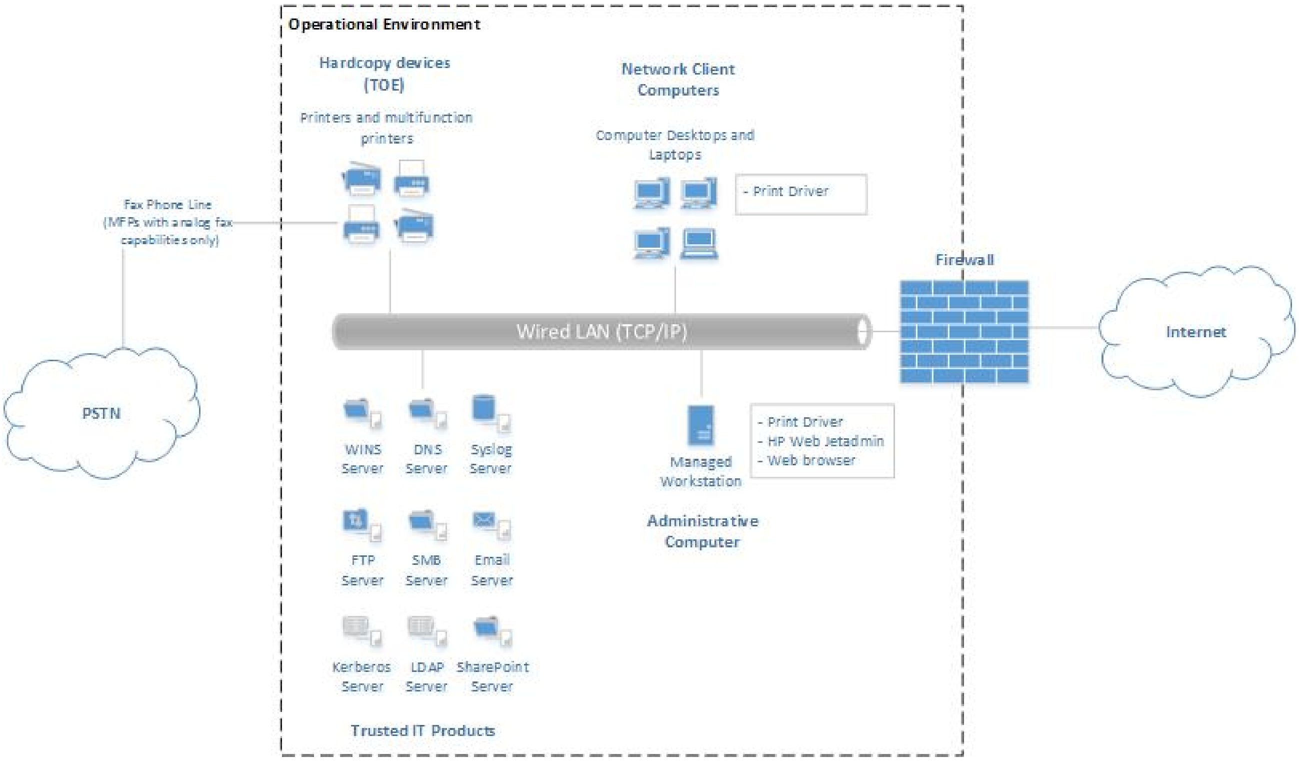

Figure 1: Typical customer environment

As discussed in section 1.4.2, the TOE is not intended to be connected to the Internet. Figure 1 shows the network, to which the TOE is connected, behind a firewall.

1.4.2 Intended method of use

This Security Target (ST) is for a commercial information processing environment in which a moderate level of document security, network security, and security assurance are required.

The TOE is intended to be used in non-hostile, networked environments where TOE users have direct physical access to the HCDs for printing, copying, faxing, scanning, and storing documents. The physical environment should be reasonably controlled and/or monitored where physical tampering of the HCDs would be evident and noticed.

The TOE is intended to be attached to a local area network using HP's Jetdirect Inside in the evaluated configuration. The evaluated configuration uses secure network mechanisms for communication between the network computers and the TOE. The TOE is managed by one designated Administrative Computer. The TOE is not intended to be connected to the Internet.

The evaluated configuration contains a built-in user identification and authentication database (a.k.a. sign-in method) used for Local Device Sign In that is part of the TOE. It also supports a Windows domain controller (via Kerberos) for a feature called Windows Sign In and a LDAP authentication server for a feature called LDAP Sign In to identify and authenticate users. The Windows domain controller and LDAP server are part of the Operational Environment.

The evaluated configuration supports the Embedded Web Server (EWS) interface for managing the TOE using a web browser over HTTP. (Web browsers are part of the Operational Environment.)

The Universal Serial Bus (USB) ports are disabled in the evaluated configuration.

1.5 TOE Description

1.5.1 TOE architecture

The TOE firmware contains intrusion detection functionality designed to detect modifications to execute in-place (XIP) code. XIP code is defined as the code in the kernel that is built to execute from a specific location in memory, and this location cannot be changed at runtime. When the TOE is initially loaded, it verifies the signatures of the loaded components to ensure that the TOE has not been modified. Once loaded, the intrusion detection code continuously scans the XIP code looking for modifications. Upon detecting a modification, the TOE attempts to perform the following notifications.

- Generate and forward an audit record to the syslog server (if a syslog server is configured)
- Create an entry in the event log stored in the TOE
- Display an error message on the Control Panel

In addition, the TOE will attempt to perform the following actions.

- Take the device offline
- Initiate a reboot of the TOE
- Upon restart of the system, and depending on an administrator configurable auto-recovery option, either halt the boot process in the Basic Input/Output System (BIOS) awaiting human confirmation or continue into a full reboot of the TOE

The intrusion detection functionality, along with the printing, copying, scanning, faxing, and storing of documents, is a standard part of the HCD firmware.

Figure 2 shows a high-level physical diagram of an HCD. The large box labeled Hardcopy Device represents the physical boundary of an HCD. The light blue shaded areas labeled Operating System, System Firmware, and Jetdirect Inside Firmware represent the TOE boundary.

The TOE connects to the local network through the Jetdirect Inside's embedded Ethernet controller (RJ45 connector), to an analog phone line (i.e., Public Switched Telephone Network (PSTN)) using the HCD's internal analog fax modem (RJ11 connector), or to a USB device using the HCD's USB ports (but the use of which must be disabled in the evaluated configuration). Some HCDs also contain a Foreign Interface Harness (FIH) port used for third-party devices that is disabled in the evaluated configuration.

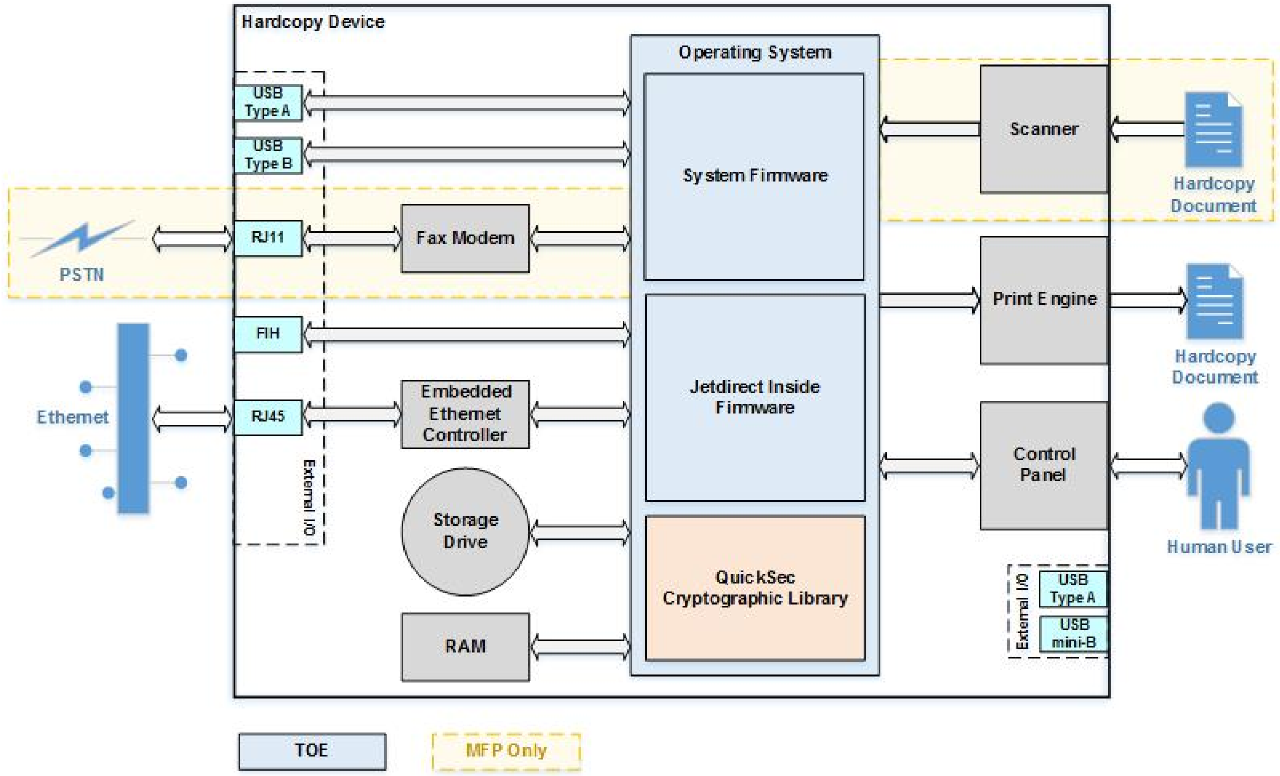

Figure 2: HCD physical diagram

The TOE is managed by a single Administrative Computer. The Administrative Computer connects to the TOE over Ethernet using IPsec with X.509v3 certificates for both mutual authentication and for protection of data from disclosure and modification. This computer can administer the TOE using the following interfaces over the IPsec connection.

- EWS
- SNMP
- Web Services:
    - OXPd Web Services
    - WS* Web Services

The HTTP-based EWS administrative interface allows an administrator to remotely manage the features of the TOE using a web browser.

The Web Services allows an administrator to remotely manage the TOE over the network. The TOE supports both HP's OXPd Web Services and certain WS* Web Services (conforming to the WS* standards defined by w3.org) accessed via the SOAP and XML.

The SNMP network interface allows an administrator to remotely manage the TOE using external SNMP-based administrative applications. The evaluated configuration supports the following SNMP versions.

- SNMPv1 read-only
- SNMPv2c read-only

- SNMPv3

Printer Job Language (PJL) is used in a non-administrative capacity by the Administrative Computer. The Administrative Computer uses PJL to send print jobs to the TOE as well as to receive job status. In general, PJL supports password protected administrative commands, but in the evaluated configuration these commands are disabled. For the purposes of this ST, we define the PJL Interface as PJL data sent to port 9100.

The TOE protects all network communications with IPsec, which is part of the embedded Jetdirect Inside Firmware. Though IPsec supports multiple authentication methods, in the evaluated configuration both ends of the IPsec connection are authenticated using X.509v3 certificates. An identity certificate for the TOE must be created outside the TOE, signed by a Certificate Authority (CA), and imported (added) into the TOE with the CA's certificate.

Because IPsec authenticates the computers (IPsec authenticates the computer itself; IPsec does not authenticate the individual users of the computer), access to the Administrative Computer should be restricted to TOE administrators only.

The TOE distinguishes between the Administrative Computer and other computers by using IP addresses, IPsec, and the embedded Jetdirect Inside's internal firewall. In the evaluated configuration, the number of Administrative Computers used to manage the TOE is limited to one and the Device Administrator Password must be set.

The TOE also supports Microsoft SharePoint (*flow* MFP models only) and remote file systems for the storing of scanned documents. The TOE uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate to SharePoint and the remote file systems. For remote file system connectivity, the TOE supports the FTP and SMB protocols. (SharePoint is HTTP-based.)

Some HCD models containing the TOE can be used to email scanned documents, email received faxes, or email sent faxes. The TOE can send email alert messages to administrator-specified email addresses, or send automated emails regarding product configuration and HCD supplies to HP. The TOE supports protected communications between the TOE and SMTP gateways. It uses IPsec with X.509v3 certificates to protect the communications and to mutually authenticate with the SMTP gateway. The TOE can only protect unencrypted email up to the SMTP gateway. It is the responsibility of the Operational Environment to protect emails from the SMTP gateway to the email's destination. Also, the TOE can only send emails; it does not accept inbound emails.

Each HCD contains a user interface called the Control Panel. The Control Panel consists of either a touchscreen LCD or a 4-line display (depending on the HCD model), a physical power button, and a physical home screen button that are attached to the HCD. In addition, *flow* MFP models include a pull-out keyboard as part of the Control Panel. The Control Panel is the physical interface that a user uses to communicate with the TOE when physically using the HCD. The touchscreen LCD displays information such as menus and status to the user. It also provides virtual buttons to the user such as an alphanumeric keypad for entering usernames and passwords. The 4-line display displays status to the user.

The TOE's Control Panel supports both local and remote sign-in methods (a.k.a. internal and external authentication mechanisms). The local sign-in method is called Local Device Sign In which supports the Device Administrator account (a.k.a. Administrator Access Code) in the evaluated configuration. This account's information is maintained in the Local Device Sign In database within the TOE. The remote sign-in methods are called LDAP Sign In and Windows Sign In (i.e., Kerberos). The TOE uses IPsec with X.509v3 certificates to protect both the LDAP and Kerberos communications.

The Scanner in Figure 2 converts hardcopy documents into electronic form. The Print Engine in Figure 2 converts electronic documents into hardcopy form.

All HCD models contain a persistent storage drive (a.k.a. storage drive) and RAM, both of which reside in the Operational Environment.

The TOE supports the auditing of security relevant functions by generating and forwarding audit records to a remote syslog server. The TOE uses IPsec with X.509v3 certificates to protect the communications between itself and the syslog server and for mutual authentication of both endpoints.

The Jetdirect Inside Firmware includes SNMP, IPsec, a firewall, and the management functions for managing these network-related features. The Jetdirect Inside Firmware also provides the network stack and drivers controlling the TOE's Ethernet interface.

The System Firmware controls the overall functions of the TOE from the Control Panel to the storage drive to the print jobs.

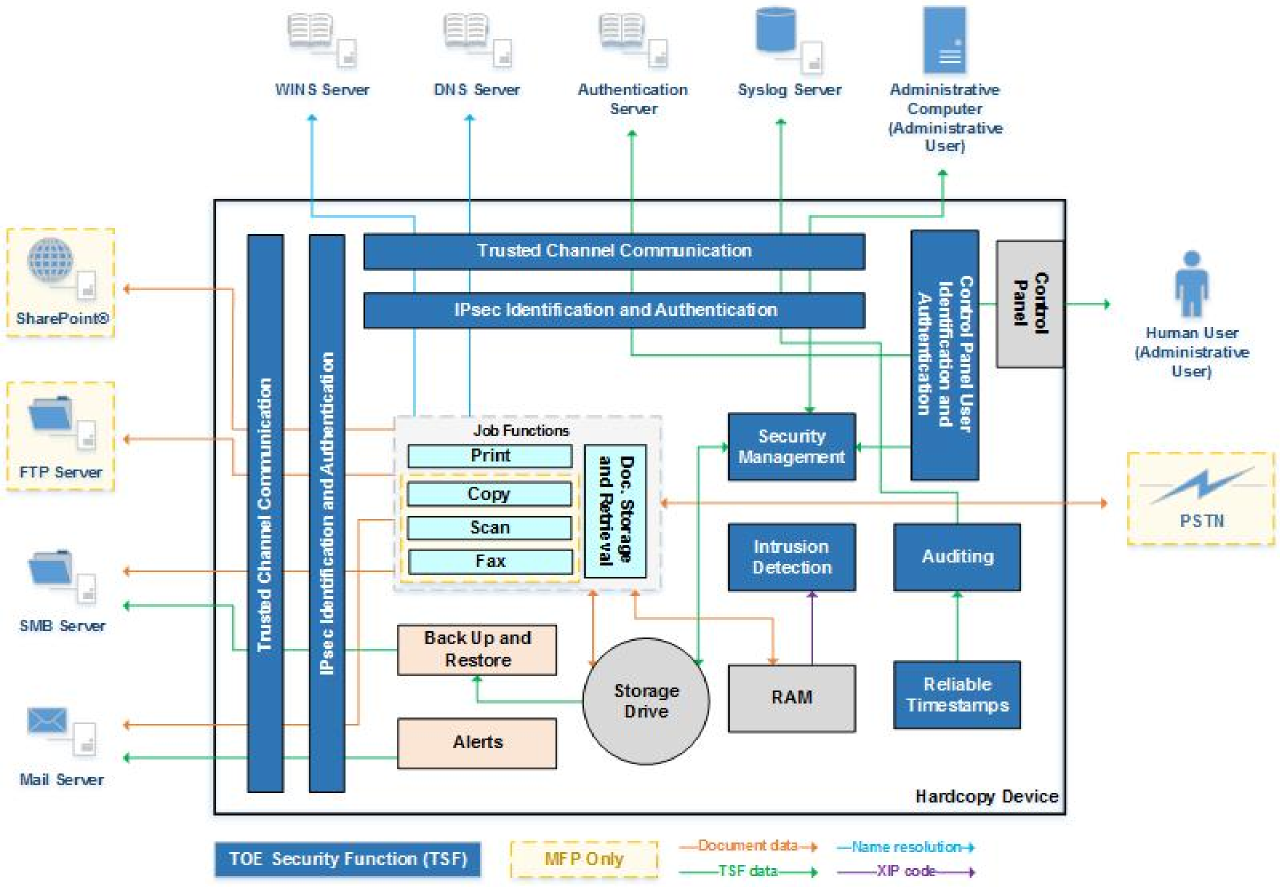
WINS Server
DNS Server
Authentication Server
Syslog Server
Administrative Computer (Administrative User)
SharePoint®
FTP Server
SMB Server
Mail Server
Human User (Administrative User)
PSTN
Trusted Channel Communication
IPsec Identification and Authentication
Trusted Channel Communication
IPsec Identification and Authentication
Control Panel User Identification and Authentication
Control Panel
Job Functions
Print
Copy
Scan
Fax
Doc. Storage and Retrieval
Security Management
Intrusion Detection
Auditing
Back Up and Restore
Alerts
Storage Drive
RAM
Reliable Timestamps
Hardcopy Device
TOE Security Function (TSF)
MFP Only
Document data
Name resolution
TSF data
XIP code

Figure 3: HCD logical diagram

Figure 3 shows a high-level logical diagram of an HCD. The large box labeled Hardcopy Device represents the logical boundary of an HCD. The dark blue shaded boxes represent the logical TOE security functions. These boxes are labeled as follows.

- Auditing
- Control Panel User Identification and Authentication

- IPsec Identification and Authentication (appears twice)
- Intrusion Detection
- Reliable Timestamps
- Security Management
- Trusted Channel Communication (appears twice)

The Jetdirect Inside Firmware provides the network connectivity and network device drivers used by the System Firmware. The System Firmware and Jetdirect Inside Firmware share the same operating system (which is part of the TOE). The System Firmware also includes internal Control Panel applications that drive the functions of the TOE. Both firmware components work together along with the OS to provide the security functionality defined in this document for the TOE.

The TOE can notify the administrator via an email alert when an event like a paper jam interrupts device usage. This is handled by the Alerts function shown in Figure 3. Additionally, the TOE can save its configuration to a file and restore its configuration from a file. This is handled by the "Back Up and Restore" function shown in the diagram.

1.5.2 TSF summary

1.5.2.1 Auditing

The TOE performs auditing of security relevant functions. Both the Jetdirect Inside Firmware and System Firmware generate audit records. The TOE connects and sends audit records to a syslog server for long-term storage and audit review. (The syslog server is part of the Operational Environment.)

1.5.2.2 Cryptography

The TOE uses IPsec to protect its communications channels. The QuickSec cryptographic library, which is part of the Operational Environment, is used to supply the cryptographic algorithms for IPsec. See section 1.5.2.6 for more information.

The TOE's XIP code protection functionality uses the Message Digest 5 (MD5) message digest algorithm to perform integrity checks on the XIP code. This algorithm is inside the TOE boundary. See section 1.5.2.4.1 for more information.

1.5.2.2.1 Cryptography outside the scope of the TOE

This section exists to inform the reader that the HCD contains other cryptography that is outside the scope of the TOE and is **not** part of this evaluation.

The product includes the ability to decrypt print jobs encrypted using the Job Encryption Password of the HP Universal Print Driver. This encryption functionality is **not** part of the claimed security functions of the TOE.

The product includes functionality to encrypt certain types of scan jobs using the Adobe PDF specification. This encryption functionality is **not** part of the claimed security functions of the TOE. Instead, the TOE uses IPsec to protect its communication channels.

The product includes functionality to encrypt email using Secure/Multipurpose Internet Mail Extensions (S/MIME) and X.509v3 certificates. This encryption functionality is **not** part of the claimed security functions of the TOE. Instead, the TOE uses IPsec to protect its communications channels.

Some HCD models contain an HP High Performance Secure Hard Disk. The HP High Performance Secure Hard Disk provides hardware-based cryptography and persistent storage to securely manage sensitive print data. Data on this drive is encrypted and the encryption key is locked to the device. The cryptographic functionality is transparent to the TOE and to the user. Not all HCD models in this evaluation contain this drive. The HCD models that do not, instead contain either an embedded MultiMediaCard (eMMC) or a Solid State Drive (SSD).

Customer data (which includes stored jobs) stored on an eMMC or SSD is encrypted under the control of the TOE using the HCD's hardware. Each time the TOE is power cycled, the cryptographic keys are destroyed and new keys are generated to encrypt the storage drive. Because of this, the jobs in Job Storage are effectively erased upon power-cycling the HCD.

1.5.2.3 Identification and authentication (I&A)

1.5.2.3.1 Control Panel I&A

The HCD has a Control Panel used to identify and authenticate users as well as to select a function (a.k.a. Control Panel application) to be performed. The Control Panel supports both local and remote sign-in methods (a.k.a. internal and external authentication mechanisms).

The local sign-in method, which is part of the TOE firmware, supported in the evaluated configuration is:

- Local Device Sign In

The remote sign-in methods, which are part of the Operational Environment, supported in the evaluated configuration are:

- LDAP Sign In
- Windows Sign In (via Kerberos)

Although the Local Device Sign In method supports multiple accounts, only the built-in Device Administrator account is to be used with this method in the evaluated configuration. The administrator must not create any Local Device Sign In accounts (a.k.a. User Access Codes).

The built-in Device Administrator account contains a display name (admin) used as an identifier and an Administrator Access Code used as the authenticator. The Administrator Access Code can be up to 16 characters in length, composed of letters, numbers, and special characters, and can be modified by an administrator.

The remote sign-in methods both use a username and password as the user account's identifier and authenticator, respectively. Each remote sign-in method determines the username and password character composition characteristics.

Control Panel user roles are determined by permission sets. The Control Panel uses permissions to determine which Control Panel applications a user can access. Each Control Panel application requires one or more permissions in order to execute it. Each Control Panel user has one or more permission sets associated with their account. The user's combined permission sets determines the user's role when logged in.

For all Control Panel account types, the permission set (PS) data are stored in the TOE and managed via EWS and WS* Web Services. The default administrative permission set in the evaluated configuration is the Device Administrator PS.

The built-in Device Administrator account has the Device Administrator PS permanently assigned to it. Summing up, the Device Administrator account has the following security attributes that are maintained by the TOE.

- Display name (admin)
- Administrator Access Code (up to 16 characters)
- Permission set (permanently set to Device Administrator PS)

Each remote sign-in account (a.k.a. network user account) contains the following security attributes.

- Username (maintained by the Operational Environment)
- Password (maintained by the Operational Environment)
- Groups (maintained by the Operational Environment)
- Permission set (maintained by the TOE)

When a user signs in through the Control Panel, the TOE displays either asterisks or dots—depending on the HCD model—for each character entered of the Administrator Access Code and remote sign-in password to prevent onlookers from viewing another user's authentication data.

Prior to signing in, the Control Panel allows users to perform certain functions such as selecting a sign-in method. Section 7.1.3.1 contains the list of functions allowed prior to signing on.

1.5.2.3.1.1 Permission sets

Permission sets are used to determine which Control Panel applications a Control Panel user can access. A permission set contains a list of allowed permissions.

The TOE contains the following built-in permission sets.

- Device Administrator—Grants administrative capabilities
- Device User—Grants typical user capabilities
- Device Guest—Grants capabilities to non-logged on users

Alternatively, administrators can create and manage custom permission sets that allow an administrator to better map the TOE's permissions to the usage model of their organization.

All permission sets are stored and maintained locally on the TOE for both the Local Sign In method and the remote sign-in methods. For more complete information on permission sets, see section 7.1.3.1.1.

1.5.2.3.1.1.1 Local Device Sign In method session permission set

For the Local Device Sign In method, the evaluated configuration only supports the local Device Administrator account. This account has the Device Administrator PS permanently assigned to it; thus, its session permission set is always equal to the Device Administrator PS.

1.5.2.3.1.1.2 Remote sign-in method session permission set

When a network user logs in to the TOE, the user's session permission set is determined using the formulas found in section 7.1.3.1.1.2. Each remote sign-in method has a permission set associated with it. Each network user account can have zero or one permission set associated with it. Each network user account can be associated with zero or more network groups. Each network group has can have zero or one permission set associated with it. The user's session permission set may include the network user account's permission set, a permission set based on the set of network groups for which the user is a member, or the remote sign-in method's permission set. The TOE uses the user's session permission set to determine the user's access to TOE functions.

1.5.2.3.1.2 Account Lockout

The Control Panel contains two account lockout mechanisms. One mechanism is used for the local Device Administrator account. The other mechanism is used for all other Control Panel account types.

For the Device Administrator account, the Control Panel counts the administrator-specified number of failed login attempts within a time interval and locks the account for an administrator-specified period of time.

For the other Control Panel account types, the Control Panel interface contains a mechanism called Simplified Account Lockout that slows Control Panel login attempts when multiple unsuccessful authentication attempts occur. It uses a combination of delays and failed attempt counts to slow login attempts.

For additional details on both account lockout mechanisms, see section 7.1.3.1.2.

1.5.2.3.2 IPsec I&A

An administrator can remotely connect to the TOE to manage the TOE. The TOE uses IPsec to identify and mutually authenticate an Administrative Computer that attempts to connect to the TOE. Since IPsec is a device-to-device protocol, the authentication occurs at the computer level, not the user level.

The TOE uses IP addresses to identify the Administrative Computer and Rivest-Shamir-Adleman (RSA) X.509v3 certificates to authenticate the Administrative Computer. The IP address of a connecting computer must be defined to the TOE's IPsec/Firewall in order for the computer to be considered authorized to access the TOE. Any computer not defined to the TOE's IPsec/Firewall is considered unauthorized and is blocked by the firewall from accessing the TOE.

The TOE uses IPsec/Firewall address templates, service templates, and rules to map IP addresses to network service protocols. An address template contains one or more IP addresses. A service template contains one or more allowed network service protocols. A rule contains a mapping of an address template to a service template. Through the rules, an administrator determines which computer is the Administrative Computer. In the evaluated configuration, the IPsec/Firewall only allows the Administrative Computer to connect to all interfaces supported by the TOE.

The TOE protects the following network interface protocols using IPsec.

- EWS (HTTP)
- OPXd
- WS*
- SNMP
- PJL

Because IPsec mutual authentication is performed at the computer level, not the user level, the computer allowed by the firewall to access the TOE via EWS, OXPd, WS*, and SNMP must itself be the Administrative Computer. This means that non-administrative users should not be allowed to logon to the Administrative Computer because every user of the Administrative Computer is potentially a TOE administrator.

IPsec is configured to use X.509v3 certificates via the Internet Key Exchange (IKE) protocols IKEv1 and IKEv2 in the evaluated configuration.

In addition, the TOE can contact many types of trusted IT products using IPsec and mutual authentication over the interfaces specified in section 7.1.6. The TOE contacts these computers either to send data to them (e.g., send email notification to the SMTP Gateway) or to request information from them (e.g., authenticate a user using LDAP). The TOE mutually authenticates these servers via IPsec prior to sending data to them and requesting information from them.

1.5.2.4 Protection of the TSF

1.5.2.4.1 Intrusion detection

Once the TOE is instantiated, the TOE runs continuous, cryptographic integrity checks on XIP. Failing one or more of these integrity checks may indicate a possible tampering of the code, thus, it may indicate an intrusion or an attack by someone attempting to violate the TOE's security policy. If the TOE detects an intrusion from the failure of one or more of these integrity checks, the TOE will attempt to perform the following notifications.

- Generate and forward an audit record to the syslog server (if a syslog server is configured)
- Create an entry in the event log stored in the TOE
- Display an error message on the Control Panel

In addition, the TOE will attempt to perform the following actions.

- Take device offline
- Initiate a reboot of the TOE
- Upon restart of the system and depending on an administrator configurable auto-recovery option, either halt the boot process in the BIOS awaiting human confirmation or continue into a full reboot of the TOE

Depending on the extent of the intrusion or attack, the TOE may or may not be able to perform one or more of these actions.

1.5.2.4.2 Reliable timestamps

The TOE contains a system clock that is used to generate reliable timestamps.

1.5.2.5 TOE access protection

1.5.2.5.1 Inactivity timeout

The Control Panel supports an inactivity timeout in case users forget to logout of the Control Panel after logging in.

1.5.2.6 Trusted channel communication and certificate management

The TOE supports IPsec to protect data being transferred over the network connections between the TOE and other trusted IT products to which the TOE connects (e.g., syslog server, SMTP gateway). IPsec along with IKE use Diffie-Hellman (DH) key establishment (a.k.a. key exchange) to establish the key used for the secure channel, IP addresses and RSA X.509v3 certificates to identify and authenticate the endpoint, and the Advanced Encryption Standard (AES) with cipher block chaining (CBC) to protect the data transfers between the TOE and the endpoint using the key derived from the key establishment. DH uses the Digital Signature Algorithm (DSA) for key generation. In addition, the Secure Hash Algorithm (SHA) and Hashed Message Authentication Code (HMAC) based on SHA are used as part of the IPsec/IKE protocol. A deterministic random bit generator (DRBG)—specifically the counter DRBG CTR_DRBG(AES) that uses AES—is used to generate cryptographically random numbers for creating encryption keys, key material, and secret keys.

The IPsec and IKE cryptographic algorithms are all supplied by the QuickSec cryptographic library. The QuickSec cryptographic library is part of the Operational Environment, but the TOE controls the usage of these algorithms.

In the evaluated configuration, the following IPsec cryptographic algorithms are supported.

- DH (IKEv1, IKEv2) key establishment/exchange (Operational Environment)
- DSA 2048-bit key pair generation (Operational Environment)
- RSA 2048-bit and 3072-bit signature generation and verification (Operational Environment)
- AES-128, AES-192, and AES-256 in CBC mode for data transfers (Operational Environment)
- AES-256 (with ECB mode) for the CTR_DRBG(AES) (Operational Environment)
- CTR_DRBG(AES) (Operational Environment)
- SHA-1, SHA-256, SHA-384, and SHA-512 hashing (Operational Environment)
- HMAC-SHA1-96 (Operational Environment)
- HMAC-SHA-256-128 (Operational Environment)
- HMAC-SHA-384-192 (Operational Environment)
- HMAC-SHA-512-256 (Operational Environment)

In addition, the TOE provides certificate management functions used to manage (add, replace, delete) X.509v3 certificates.

1.5.2.7 Security management

The TOE provides management capabilities for managing its security functionality. The TOE supports the following role.

- Administrators

Administrators have the authority to manage the security functionality of the TOE. For more detail on security management, see section 7.1.7.

1.5.3 TOE boundaries

1.5.3.1 Physical

The physical boundary of the TOE is the programs and data stored in the System Firmware and Jetdirect Inside Firmware of the HCD (except for the QuickSec cryptographic library) and the English-language guidance documentation.

It is typical for an HCD, and thus the TOE, for users to have direct physical access to the HCD. By design, users have easy access to some of the hardware features, such as the Control Panel, the paper input trays, the printer output trays, the scanner, and the power button. But other features such as the processor, volatile memory, and storage drive are located inside the HCD in the formatter cage. The formatter cage can be secured to the HCD chassis using a combination lock, thus, restricting normal user access to the components inside the cage.

Due to the physical accessibility of the HCDs, they must be used in non-hostile environments. Physical access should be controlled and/or monitored.

QuickSec version 5.1 ([QuickSec51]) toolkit implements the TOE's IPsec including the IPsec/Firewall. The QuickSec toolkit includes a cryptographic library (a.k.a. encryption library) and an IPsec library. Although the QuickSec IPsec library is in the TOE boundary, the QuickSec cryptographic library used by QuickSec for all IPsec cryptography is part of the Operational Environment.

QuickSec is developed and tested by INSIDE Secure. The QuickSec cryptographic algorithms used by the TOE where tested during the evaluation against a reference implementation of IPsec.

Regarding the SMTP gateway, the TOE can only provide protection of sent emails to the device with which the TOE has the IPsec connection (i.e., the TOE only provides protection between the TOE and SMTP gateway). After that point, the Operational Environment must provide the remaining protection necessary to transfer the email from the SMTP gateway to the email's addressee(s).

The following table lists the English-language guidance documentation for the TOE.

Title	Edition
Common Criteria Evaluated Configuration Guide for HP Enterprise LaserJet, Officejet, and PageWide Single-Function and Multifunction Printers running HP FutureSmart Firmware with Intrusion Detection	1, 1/2019
Practical IPsec Deployment for Printing and Imaging Devices whitepaper (http://www1.hp.com/ctg/Manual/c01048192)	June 2008
HP PageWide Enterprise Color 556 User Guide	1, 5/2016
HP PageWide Enterprise Color MFP 586 User Guide (includes Flow)	1, 5/2016
HP LaserJet Enterprise M506 User Guide	2, 8/2017
HP LaserJet Enterprise 500 MFP M525 User Guide	1, 8/2017
HP LaserJet Enterprise Flow MFP M525c User Guide	1, 8/2017
HP LaserJet Enterprise MFP M527 User Guide (includes Flow)	2, 8/2015
HP Color LaserJet Enterprise M552/M553 User Guide	1, 11/2015
HP LaserJet Enterprise 500 Color MFP M575 User Guide	1, 5/2012
HP LaserJet Enterprise Color Flow MFP M575 User Guide	2, 11/2012
HP Color LaserJet Enterprise MFP M577 User Guide (includes Flow)	1, 11/2015
HP LaserJet Enterprise M604, M605, M606 User Guide	2, 8/2017
HP LaserJet Enterprise MFP M630 User Guide (includes Flow)	2, 8/2017
HP Color LaserJet Enterprise M651 User Guide	1, 11/2015
HP Color LaserJet Enterprise MFP M680 User Guide (includes Flow)	1, 11/2015
HP LaserJet Enterprise MFP M725 User Guide	2, 8/2017

Title	Edition
HP LaserJet Enterprise Flow MFP M830 User Guide	2, 8/2017
HP Color LaserJet Enterprise M855 User Guide	1, 11/2015
HP Color LaserJet Enterprise Flow MFP M880 User Guide	1, 11/2015
HP Officejet Enterprise Color X555 User Guide	1, 4/2014
HP Officejet Enterprise Color MFP X585/Flow X585 User Guide	1, 11/2015

Table 2: English-only guidance documentation

1.5.3.2 Logical

The security functionality provided by the TOE has been described above and includes:

- Auditing,
- Cryptography,
- Identification and authentication,
- Protection of the TSF,
- TOE access protection,
- Trusted channel communication and certificate management, and
- Security management.

1.5.3.3 Evaluated configuration

The following items will need to be adhered to in the evaluated configuration.

- HP Digital Sending Software (DSS) must be disabled
- Device Administrator Password must be set as per P.ADMIN.PASSWORD
- Only one Administrative Computer is used to manage the TOE
- HP and third party applications cannot be installed on the TOE
- All received faxes must be stored in Job Storage
- Fax Forwarding and Fax Archiving must be disabled
- PC Fax Send must be disabled
- Device USB and Host USB plug and play must be disabled
- FIH port must be disabled
- Remote Firmware Upgrade through any means other than EWS (e.g., PJL) and USB must be disabled
- Jetdirect Inside management via telnet and FTP must be disabled
- Jetdirect XML Services must be disabled
- External file system access through PJL and PostScript (PS) must be disabled
- IPsec authentication using X.509v3 certificates must be enabled (IPsec authentication using Kerberos or Pre-Shared Key is not supported)
- IPsec Authenticated Headers (AH) must be disabled

- Full Authentication must be enabled (this disables the Guest role)
- SNMP support limited to:
  - SNMPv1 read-only
  - SNMPv2c read-only
  - SNMPv3
- The Service PIN, used by a customer support engineer to access functions available to HP support personnel, must be disabled
- Near Field Communication (NFC) must be disabled
- Wireless Direct Print must be disabled
- PJL device access commands must be disabled
- When using Windows Sign In, the Windows domain must reject Microsoft NT LAN Manager (NTLM) connections
- The "Save to HTTP" function is disallowed and must not be configured to function with an HTTP server
- Display Names for the Local Device Sign In method users and user names for the LDAP and Windows Sign In method users must only contain the characters defined in P.USERNAME.CHARACTER_SET.
- Remote Control-Panel use is disallowed per P.REMOTE_PANEL.DISALLOWED
- User Access Codes use is disallowed.

1.5.4 Security policy model

This section describes the security policy model for the TOE.

1.5.4.1 Subjects/Users

The user role defined for the TOE is: administrator.

There are two types of users.

- **Control Panel users**—Administrative users who physically access the TOE's Control Panel
  - **Security attributes**: User role (defined by session permission sets) and user identifier
- **IPsec users**—Administrative Computers that can successfully authenticate to the TOE's administrative interfaces (e.g., EWS/HTTP, OXPd, WS*, SNMP) and the PJL interface using IPsec and mutual authentication.
  - **Security attributes:** User role (defined by IPsec/Firewall service template) and user identifier (define by IP address)

1.5.4.2 Objects

The following objects are protected by the TOE.

- TSF data

TSF data objects are:

- Administrator I&A and role data,
- Audit records,
- Cryptographic keys and certificates,

- Device and network configuration settings (including IPsec/Firewall rules and templates),
- Inactivity timeout data,
- Simplified account lockout data, and
- System time.

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL2, augmented by ALC_FLR.2.

This Security Target does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 5 is the basis for this conformance claim.

3 Security Problem Definition

3.1 Introduction

The statement of TOE security environment describes the security aspects of the environment in which the TOE is intended to be used and the manner in which it is expected to be deployed.

To this end, the statement of TOE security environment identifies the list of assumptions made on the Operational Environment (including physical and procedural measures) and the intended method of use of the product, defines the threats that the product is designed to counter, and the organizational security policies with which the product is designed to comply.

3.2 Threat Environment

This security problem definition addresses threats posed by the following 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, and

e) Persons who are unauthorized to use the TOE's administrative functions who may attempt to modify (corrupt or inject malware) the TSF XIP code.

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

The threat agents are assumed to originate from a well-managed user community in a non-hostile working environment. Therefore, the product protects against threats of security vulnerabilities that might be exploited in the intended environment for the TOE with low level of expertise and effort. The TOE protects against straightforward or intentional breach of TOE security by attackers possessing a Basic attack potential.

3.2.1 Threats countered by the TOE

T.TSF_DATA.IN_TOE_DIS

TSF data in the TOE may be disclosed by unauthorized persons.

T.TSF_DATA.IN_TOE_MOD

TSF data in the TOE may be modified by unauthorized persons.

T.TSF_DATA.IN_TRANSIT_DIS

TSF data on the network may be disclosed by unauthorized persons.

T.TSF_DATA.IN_TRANSIT_MOD

TSF data on the network may be modified by unauthorized persons.

T.XIP.MOD

The TOE's XIP code may be modified (corruption or injection of malware) by unauthorized persons.

3.3 Assumptions

3.3.1 Environment of use of the TOE

3.3.1.1 Physical

A.ACCESS.MANAGED

The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE.

A.ADMIN.PC.SECURE

The administrative computer is in a physically secured and managed environment and only the authorized administrator has access to it.

3.3.1.2 Personnel

A.ADMIN.TRAINING

Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures.

A.ADMIN.TRUST

Administrators do not use their privileged access rights for malicious purposes.

3.3.1.3 Connectivity

A.EMAILS.PROTECTED

For emails sent by the TOE to the SMTP gateway, the transmission of emails from the SMTP gateway to the email's destination is protected.

A.SERVICES.RELIABLE

When the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, SMTP, SharePoint, syslog, and/or WINS, these services provide reliable information and responses to the TOE.

3.4 Organizational Security Policies

P.ADMIN.AUTHORIZATION

To preserve operational accountability and security, administrators will be authorized to use the TOE only as permitted by the TOE owner.

P.ADMIN.PASSWORD

To restrict access to administrative tasks, the Device Administrator Password will be set in the evaluated configuration so that this password is required to perform security-relevant actions through EWS (HTTP), OXPd, WS* Web Services, or at the Control Panel.

P.AUDIT.LOGGING

To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created by the TOE. Exported audit records will be protected from unauthorized disclosure or modification and will be reviewed by authorized personnel.

P.INTERFACE.MANAGEMENT

To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its Operational Environment.

P.REMOTE_PANEL.DISALLOWED

To preserve operational accountability and security, administrators must not use the Remote Control-Panel feature.

P.RSA.KEYSIZE

To preserve IPsec communications security, all devices connecting to the TOE via IPsec must be configured to use an RSA key size of 2048-bits or greater.

P.USERNAME.CHARACTER_SET

To prevent ambiguous user names in the TOE's audit trail, the Display Names of the Local Device Sign In method users and the user names of the LDAP and Windows Sign In method users must only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

4 Security Objectives

4.1 Objectives for the TOE

O.ADMIN.AUTHORIZED

The TOE shall require identification and authentication of administrators, and shall ensure that administrators are authorized in accordance with security policies before allowing them to use the TOE.

O.AUDIT.LOGGED

The TOE shall generate audit data of TOE use and security-relevant events.

O.INTERFACE.MANAGED

The TOE shall manage the operation of external interfaces in accordance with security policies.

O.TSF_DATA.IN_TOE_DIS

The TOE shall protect TSF data in the TOE from unauthorized disclosure.

O.TSF_DATA.IN_TOE_MOD

The TOE shall protect TSF data in the TOE from unauthorized modification.

O.TSF_DATA.IN_TRANSIT_DIS

The TOE shall protect TSF data on the network from unauthorized disclosure.

O.TSF_DATA.IN_TRANSIT_MOD

The TOE shall protect TSF data on the network from unauthorized modification.

O.XIP.CHECKS

The TOE shall perform continuous, run-time, cryptographic integrity checks of XIP code to detect potential intrusions.

O.XIP.RESPONSE

If an integrity check of XIP code fails, the TOE shall notify of and recover from the potential intrusion.

4.2 Objectives for the Operational Environment

OE.ADMIN.AUTHORIZED

The TOE owner shall grant permission to administrators to be authorized to use the TOE according to the security policies and procedures of their organization.

OE.ADMIN.PC.SECURE

The TOE owner shall locate the Administrative Computer in a physically secured and managed environment and allow only authorized personnel access to it.

OE.ADMIN.TRAINED

The TOE owner shall ensure that TOE Administrators are aware of the security policies and procedures of their organization; have the training, competence, and time to follow the manufacturer's guidance and documentation; and correctly configure and operate the TOE in accordance with those policies and procedures.

OE.ADMIN.TRUSTED

The TOE owner shall establish trust that TOE Administrators will not use their privileged access rights for malicious purposes.

OE.AUDIT.REVIEWED

The TOE owner shall ensure that audit logs are reviewed at appropriate intervals for security violations or unusual patterns of activity.

OE.AUDIT_ACCESS.AUTHORIZED

If audit records generated by the TOE are exported from the TOE to another trusted IT product, the TOE owner shall ensure that those records can be accessed in order to detect potential security violations, and only by authorized persons.

OE.AUDIT_STORAGE.PROTECTED

If audit records are exported from the TOE to another trusted IT product, the TOE owner shall ensure that those records are protected from unauthorized access, deletion and modifications.

OE.EMAILS.PROTECTED

The Operational Environment shall protect the transmission of emails from the SMTP gateway to the email’s destination.

OE.INTERFACE.MANAGED

The Operational Environment shall provide protection from unmanaged access to TOE external interfaces.

OE.PHYSICAL.MANAGED

The TOE shall be placed in a secure or monitored area that provides protection from unmanaged physical access to the TOE.

OE.RSA.KEYSIZE

Devices connecting to the TOE via IPsec shall use an RSA key size of 2048-bits or greater.

OE.SERVICES.RELIABLE

When the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, SMTP, SharePoint, syslog, and/or WINS, these services shall provide reliable information and responses to the TOE.

OE.USERNAME.CHARACTER_SET

The Display Names of all Local Device Sign In method users and the user names of all LDAP and Windows Sign In method users shall only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.ADMIN.AUTHORIZED	T.TSF_DATA.IN_TOE_DIS T.TSF_DATA.IN_TOE_MOD T.TSF_DATA.IN_TRANSIT_DIS T.TSF_DATA.IN_TRANSIT_MOD P.ADMIN.AUTHORIZATION
O.AUDIT.LOGGED	P.AUDIT.LOGGING
O.INTERFACE.MANAGED	P.INTERFACE.MANAGEMENT
O.TSF_DATA.IN_TOE_DIS	T.TSF_DATA.IN_TOE_DIS
O.TSF_DATA.IN_TOE_MOD	T.TSF_DATA.IN_TOE_MOD
O.TSF_DATA.IN_TRANSIT_DIS	T.TSF_DATA.IN_TRANSIT_DIS
O.TSF_DATA.IN_TRANSIT_MOD	T.TSF_DATA.IN_TRANSIT_MOD
O.XIP.CHECKS	T.XIP.MOD
O.XIP.RESPONSE	T.XIP.MOD

Table 3: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.ADMIN.AUTHORIZED	T.TSF_DATA.IN_TOE_DIS T.TSF_DATA.IN_TOE_MOD T.TSF_DATA.IN_TRANSIT_DIS T.TSF_DATA.IN_TRANSIT_MOD P.ADMIN.AUTHORIZATION
OE.ADMIN.PC.SECURE	A.ADMIN.PC.SECURE
OE.ADMIN.TRAINED	A.ADMIN.TRAINING P.ADMIN.PASSWORD P.REMOTE_PANEL.DISALLOWED
OE.ADMIN.TRUSTED	A.ADMIN.TRUST
OE.AUDIT.REVIEWED	P.AUDIT.LOGGING

Objective	Assumptions / Threats / OSPs
OE.AUDIT_ACCESS.AUTHORIZED	P.AUDIT.LOGGING
OE.AUDIT_STORAGE.PROTECTED	P.AUDIT.LOGGING
OE.EMAILS.PROTECTED	A.EMAILS.PROTECTED
OE.INTERFACE.MANAGED	P.INTERFACE.MANAGEMENT
OE.PHYSICAL.MANAGED	A.ACCESS.MANAGED
OE.RSA.KEYSIZE	P.RSA.KEYSIZE
OE.SERVICES.RELIABLE	A.SERVICES.RELIABLE
OE.USERNAME.CHARACTER_SET	P.USERNAME.CHARACTER_SET

Table 4: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat.

Threat	Rationale for security objectives
T.TSF_DATA.IN_TOE_DIS	The threat: ● TSF data in the TOE may be disclosed by unauthorized persons. is countered by: ● O.TSF_DATA.IN_TOE_DIS which protects TSF data in the TOE from unauthorized disclosure. ● O.ADMIN.AUTHORIZED which establishes administrator identification and authentication as the basis for authorization. ● OE.ADMIN.AUTHORIZED which establishes responsibility of the TOE owner to appropriately grant authorization.
T.TSF_DATA.IN_TOE_MOD	The threat: ● TSF data in the TOE may be modified by unauthorized persons. is countered by: ● O.ADMIN.AUTHORIZED which establishes administrator identification and authentication as the basis for authorization. ● O.TSF_DATA.IN_TOE_MOD which protects TSF data in the TOE from unauthorized modification. ● OE.ADMIN.AUTHORIZED which establishes responsibility of the TOE owner to appropriately grant authorization.
T.TSF_DATA.IN_TRANSIT_DIS	The threat:

Threat	Rationale for security objectives
	● TSF data on the network may be disclosed by unauthorized persons. is countered by: ● O.ADMIN.AUTHORIZED which establishes administrator identification and authentication as the basis for authorization. ● O.TSF_DATA.IN_TRANSIT_DIS which protects TSF data on the network from unauthorized disclosure. ● OE.ADMIN.AUTHORIZED which establishes responsibility of the TOE owner to appropriately grant authorization.
T.TSF_DATA.IN_TRANSIT_MOD	The threat: ● TSF data on the network may be modified by unauthorized persons. is countered by: ● O.ADMIN.AUTHORIZED which establishes administrator identification and authentication as the basis for authorization. ● O.TSF_DATA.IN_TRANSIT_MOD which protects TSF data on the network from unauthorized modification. ● OE.ADMIN.AUTHORIZED which establishes responsibility of the TOE owner to appropriately grant authorization.
T.XIP.MOD	The threat: ● The TOE's XIP code may be modified (corruption or injection of malware) by unauthorized persons. is countered by: ● O.XIP.CHECKS which requires the TOE to detect modifications in the XIP code. ● O.XIP.RESPONSE which requires the TOE to provide notification of a detected modification and to recover from the modification.

Table 5: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported.

Assumption	Rationale for security objectives
A.ACCESS.MANAGED	The assumption: ● The TOE is located in a restricted or monitored environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE. is upheld by:

Assumption	Rationale for security objectives
	● OE.PHYSICAL.MANAGED which establishes a protected physical environment for the TOE.
A.ADMIN.PC.SECURE	The assumption: ● The administrative computer is in a physically secured and managed environment and only the authorized administrator has access to it. is upheld by: ● OE.ADMIN.PC.SECURE which establishes the responsibility of the TOE owner to locate the administrative computer in a physically secured and managed environment and allow only authorized personnel access.
A.ADMIN.TRAINING	The assumption: ● Administrators are aware of the security policies and procedures of their organization, are trained and competent to follow the manufacturer's guidance and documentation, and correctly configure and operate the TOE in accordance with those policies and procedures. is upheld by: ● OE.ADMIN.TRAINED which establishes responsibility of the TOE owner to provide appropriate Administrator training.
A.ADMIN.TRUST	The assumption: ● Administrators do not use their privileged access rights for malicious purposes. is upheld by: ● OE.ADMIN.TRUSTED which establishes responsibility of the TOE owner to have a trusted relationship with Administrators.
A.EMAILS.PROTECTED	The assumption: ● For emails sent by the TOE to the SMTP gateway, the transmission of emails from the SMTP gateway to the email's destination is protected. is upheld by: ● OE.EMAILS.PROTECTED which protects the transmission of emails from the SMTP gateway to the email’s destination.
A.SERVICES.RELIABLE	The assumption: ● When the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, SMTP, SharePoint, syslog, and/or WINS, these services provide reliable information and responses to the TOE. is upheld by:

Assumption	Rationale for security objectives
	● OE.SERVICES.RELIABLE which, when the TOE uses any of the network services SMB, FTP, DNS, Kerberos, LDAP, SMTP, SharePoint, syslog, and/or WINS, establishes that these services provide reliable information and responses to the TOE.

Table 6: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy (OSP), that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented.

OSP	Rationale for security objectives
P.ADMIN.AUTHORIZATION	The OSP: ● To preserve operational accountability and security, administrators will be authorized to use the TOE only as permitted by the TOE owner. is enforced by: ● O.ADMIN.AUTHORIZED which establishes administrator identification and authentication as the basis for authorization to use the TOE. ● OE.ADMIN.AUTHORIZED which establishes responsibility of the TOE owner to appropriately grant authorization.
P.ADMIN.PASSWORD	The OSP: ● To restrict access to administrative tasks, the Device Administrator Password will be set in the evaluated configuration so that this password is required to perform security-relevant actions through EWS (HTTP), OXPd, WS* Web Services, or at the Control Panel. is enforced by: ● OE.ADMIN.TRAINED which establishes responsibility of the TOE owner to provide appropriate Administrator training.
P.AUDIT.LOGGING	The OSP: ● To preserve operational accountability and security, records that provide an audit trail of TOE use and security-relevant events will be created by the TOE. Exported audit records will be protected from unauthorized disclosure or modification and will be reviewed by authorized personnel. is enforced by: ● O.AUDIT.LOGGED which creates a log of TOE use and security-relevant events. ● OE.AUDIT_STORAGE.PROTECTED which protects exported audit records from unauthorized access, deletion and modifications.

OSP	Rationale for security objectives
	● OE.AUDIT_ACCESS.AUTHORIZED which establishes responsibility of the TOE owner to provide appropriate access to exported audit records. ● OE.AUDIT.REVIEWED which establishes responsibility of the TOE owner to ensure that audit logs are appropriately reviewed.
P.INTERFACE.MANAGEMENT	The OSP: ● To prevent unauthorized use of the external interfaces of the TOE, operation of those interfaces will be controlled by the TOE and its Operational Environment. is enforced by: ● O.INTERFACE.MANAGED which manages the operation of external interfaces in accordance with security policies. ● OE.INTERFACE.MANAGED which establishes a protected environment for TOE external interfaces.
P.REMOTE_PANEL.DISALLOWED	The OSP: ● To preserve operational accountability and security, administrators must not use the Remote Control-Panel feature. is enforced by: ● OE.ADMIN.TRAINED which establishes responsibility of the TOE owner to provide appropriate Administrator training.
P.RSA.KEYSIZE	The OSP: ● To preserve IPsec communications security, all devices connecting to the TOE via IPsec must be configured to use an RSA key size of 2048-bits or greater. is enforced by: ● OE.RSA.KEYSIZE which establishes that devices connecting to the TOE via IPsec shall use an RSA key size of 2048-bits or greater.
P.USERNAME.CHARACTER_SET	The OSP: ● To prevent ambiguous user names in the TOE's audit trail, the Display Names of the Local Device Sign In method users and the user names of the LDAP and Windows Sign In method users must only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E). is enforced by: ● OE.USERNAME.CHARACTER_SET which establishes that the Display Names of all Local Device Sign In users and the user names of all LDAP and Windows Sign In method users shall only contain ASCII printable characters except for the double quote (22 hex) and single quote (27 hex) characters (i.e., allowed ASCII characters in hexadecimal: 20, 21, 23 - 26, 28 - 7E).

Table 7: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

This section contains the extended component definition(s) used by this ST.

5.1 Class FCS: Cryptographic support

5.1.1 Cryptographic Operation (Random Bit Generation) (FCS_RBG)

Family behaviour

This family defines requirements for random bit generation to ensure that it is performed in accordance with selected standards and seeded by an entropy source

Component levelling

FCS_RBG_EXT.1 Random Bit Generation requires random bit generation to be performed in accordance with selected standards and seeded by an entropy source.

Management: FCS_RBG_EXT.1

There are no management activities foreseen.

Audit: FCS_RBG_EXT.1

There are no audit events foreseen.

5.1.1.1 FCS_RBG_EXT.1 - Random Bit Generation

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all deterministic random bit generation services in accordance with NIST SP 800-90A using [selection: **Hash_DRBG(any), HMAC_DRBG(any), CTR_DRBG(AES)**].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from software-based noise sources with a minimum of [selection: **128 bits, 256 bits**] of entropy at least equal to the greatest security strength, according to NIST SP 800-57, of the keys and hashes that it will generate.

Rationale

Random bits/number will be used by the SFRs for key generation and destruction, and the Common Criteria does not provide a suitable SFR for the random bit generation.

This extended component ensures the strength of encryption keys, and it is therefore placed in the FCS class with a single component.

5.2 Class FPT: Protection of the TSF

This section describes the functional requirements for the following features.

- TSF executable image integrity
- TSF XIP code protection

5.2.1 TSF XIP code protection (FPT_XCP)

Family behaviour

The TSF XIP code protection component refers to restrictions on unauthorized access to XIP code, and to the deterrence of, and resistance to, unauthorized XIP code modification, or substitution of the TSF. This type of modification is considered an attack or intrusion on the TSF. The detection of such a modification is commonly called intrusion detection.

The requirements of the component in this family ensure that the TSF is protected from XIP code tampering and interference. Satisfying the requirements of this component results in the TSF being instrumented and configured in such a manner that an XIP code intrusion is detectable, or resistance to XIP code intrusions is enforced. This component also provides requirements regarding how the TSF shall respond to detected XIP code intrusions. Depending on the extent of the intrusion, the TOE may not be able to perform one or more of the listed responses.

Component levelling

FPT_XCP_EXT.1 Intrusion detection and response for XIP code, provides detection functionality and attempted response functionality when an intrusion is detected by the TOE.

Management: FPT_XCP_EXT.1

The following actions could be considered for the management functions in FMT:

a) management of the response functionality;

Audit: FPT_XCP_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) Minimal: detection of intrusion.

5.2.1.1 FPT_XCP_EXT.1 - Intrusion detection and response for XIP code

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation

FPT_XCP_EXT.1.1 The TSF shall perform continuous, run-time, cryptographic integrity checks of XIP code to detect potential intrusions.

FPT_XCP_EXT.1.2 The TSF shall attempt to provide the following notifications upon detection of a potential intrusion: [assignment: **list of notifications**].

FPT_XCP_EXT.1.3 The TSF shall attempt to provide the following actions upon detection of a potential intrusion: [assignment: **list of actions**].

Rationale

Class FPT doesn't have a specific family of security functional requirements (SFRs) for detecting modifications of executing firmware/software such as XIP code. The FPT_XCP_EXT family is similar to the FPT_PHP family in that it focuses on attacks, but FPT_PHP focuses specifically on physical security. In addition, the FPT_XCP_EXT family allows for specifying a set of attempted responses by the TOE when an intrusion is detected by the TOE.

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the SFRs for the TOE, and the operations performed on the components according to CC part 1: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		CC Part 2	No	No	Yes	Yes
	FAU_GEN.2 User identity association		CC Part 2	No	No	No	No
FCS - Cryptographic support	FCS_CKM.1 Cryptographic key generation		CC Part 2	No	Yes	Yes	No
	FCS_CKM.2 Cryptographic key establishment		CC Part 2	No	Yes	Yes	No
	FCS_COP.1-ipsec Cryptographic operations for IPsec	FCS_COP.1	CC Part 2	Yes	Yes	Yes	No
	FCS_COP.1-xcp Cryptographic operation for XIP code protection	FCS_COP.1	CC Part 2	Yes	Yes	Yes	No
	FCS_RBG_EXT.1 Random Bit Generation		ECD	No	Yes	No	Yes
FIA - Identification and authentication	FIA_AFL.1 Authentication failure handling		CC Part 2	No	No	Yes	Yes
	FIA_ATD.1 Local user attribute definition		CC Part 2	No	No	Yes	No
	FIA_UAU.1 Timing of Control Panel authentication		CC Part 2	No	Yes	Yes	No
	FIA_UAU.2 IPsec authentication before any action		CC Part 2	No	Yes	No	No
	FIA_UAU.7 Control Panel protected authentication feedback		CC Part 2	No	Yes	Yes	No
	FIA_UID.1 Timing of Control Panel identification		CC Part 2	No	Yes	Yes	No
	FIA_UID.2 IPsec identification before any action		CC Part 2	No	Yes	No	No
	FIA_USB.1 User-subject binding		CC Part 2	No	No	Yes	No
FMT - Security management	FMT_MOF.1-auth Management of authentication behavior	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FMT_MOF.1-lockout Management of authentication behavior	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MTD.1-ipsec Management of IPsec TSF data	FMT_MTD.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MTD.1-misc Management of miscellaneous TSF data	FMT_MTD.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MTD.1-permset Management of permission sets	FMT_MTD.1	CC Part 2	Yes	No	Yes	Yes
	FMT_SMF.1 Specification of management functions		CC Part 2	No	No	Yes	No
	FMT_SMR.1 Security roles		CC Part 2	No	No	Yes	No
FPT - Protection of the TSF	FPT_STM.1 Reliable time stamps		CC Part 2	No	No	No	No
	FPT_XCP_EXT.1 Intrusion detection and response for XIP code		ECD	No	No	Yes	No
FTA - TOE access	FTA_SSL.3 Control Panel TSF-initiated termination		CC Part 2	No	Yes	Yes	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		CC Part 2	No	No	Yes	Yes

Table 8: SFRs for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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

a) Start-up and shutdown of the audit functions; and

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

c) **All Auditable Events as each is defined for its Audit Level (if one is specified) for the Relevant SFR in Table 9**.

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 (if applicable), 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, **for each Relevant SFR listed in Table 9: (1) information as defined by its Audit Level (if one is specified), and (2) all Additional Information (if any is required)**.

Auditable event	Relevant SFR(s)	Audit level	Additional information
Both successful and unsuccessful use of the authentication mechanism	FIA_UAU.1, FIA_UAU.2	Basic	None
Both successful and unsuccessful use of the identification mechanism	FIA_UID.1, FIA_UID.2	Basic	Attempted user identity, if available
Management of authentication behavior	FMT_MOF.1-auth	Minimum	None
Management of IPsec TSF data	FMT_MTD.1-ipsec	Minimum	None
Management of the Administrator Access Code	FMT_MTD.1-misc	Minimum	None
Modifications to the group of users that are part of a role	FMT_SMR.1	Minimum	None
Changes to the time	FPT_STM.1, FMT_MTD.1-misc (system time)	Minimum	None
Detection of tampering	FPT_XCP_EXT.1	Basic	None
Failure of the trusted channel functions	FTP_ITC.1	Minimum	None
Termination of an interactive session by the session termination mechanism	FTA_SSL.3	Minimum	None

Table 9: Auditable events

6.1.1.2 User identity association (FAU_GEN.2)

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.

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

FCS_CKM.1.1 The *QuickSec cryptographic library in the Operational Environment* ~~TSF~~ shall generate *asymmetric* cryptographic keys in accordance with a specified cryptographic key generation algorithm **defined in Table 10** and specified cryptographic key sizes **defined in Table 10** that meet the following: **the standards defined in Table 10**.

Protocol	Key generation algorithm	Key sizes	Standards
IPsec	DSA	2048-bit	[FIPS186-2]☝ Finite Field Cryptography (FFC) “Digital Signature Standard (DSS)”

Table 10: Asymmetric cryptographic key generation

Application Note: *Random bit generation for FCS_CKM.1 is implemented by FCS_RBG_EXT.1.*

6.1.2.2 Cryptographic key establishment (FCS_CKM.2)

FCS_CKM.2.1 The *QuickSec cryptographic library in the Operational Environment* ~~TSF~~ shall *perform cryptographic key establishment* ~~distribute cryptographic keys~~ in accordance with a specified cryptographic key *establishment*~~distribution~~ method **defined in Table 11** that meets the following: **the standards defined in Table 11**.

Protocol	Key establishment method	Standards
IPsec	IKEv1 (DH)	[RFC4109] Algorithms for Internet Key Exchange version 1 (IKEv1)
	IKEv2 (DH)	[RFC4306] Diffie-Hellman key agreement method defined for the IKEv2 protocol; [RFC4718] IKEv2 Clarifications and Implementation Guidelines

Table 11: Cryptographic key establishment

6.1.2.3 Cryptographic operations for IPsec (FCS_COP.1-ipsec)

FCS_COP.1.1 The *QuickSec cryptographic library in the Operational Environment* ~~TSF~~ shall perform **the operations defined in Table 12** in accordance with a specified cryptographic algorithm **defined in Table 12** and cryptographic key sizes **defined in Table 12** that meet the following: **the standards defined in Table 12**.

Protocol	Operations	Algorithm	Key sizes (in bits)	Standards
IPsec	Signature generation and verification	RSA	2048, 3072	[PKCS1v1.5] Public-Key Cryptography Standard (PKCS) #1 v1.5: RSA Encryption Standard
	Symmetric encryption and decryption	AES	CBC: 128, 192, 256; ECB: 256	[FIPS197] Advanced Encryption Standard; [SP800-38A] Recommendation for Block Cipher Modes of Operation: Methods and Techniques
	Secure hash	SHA-1, SHA-256, SHA-384, SHA-512		[FIPS180-4] Secure Hash Standard (SHS); [RFC4894] Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec
	Data authentication	HMAC-SHA1-96	160	[RFC2404] Use of HMAC-SHA1-96
		HMAC-SHA-256-128	256	[RFC4868] Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
		HMAC-SHA-384-192	384	

Protocol	**Operations**	**Algorithm**	**Key sizes (in bits)**	**Standards**
		HMAC-SHA-512-256	512	

Table 12: Cryptographic operations for IPsec

6.1.2.4 Cryptographic operation for XIP code protection (FCS_COP.1-xcp)

FCS_COP.1.1 The TSF shall perform **message digest generation** in accordance with a specified cryptographic algorithm **MD5** and cryptographic key *size* ~~sizes~~ **128-bits** that meet the following: **[RFC1321]**☝.

6.1.2.5 Random Bit Generation (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The *QuickSec cryptographic library in the Operational Environment* ~~TSF~~ shall perform all deterministic random bit generation services in accordance with NIST SP 800-90A using **CTR_DRBG(AES)**.

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from software-based noise sources with a minimum of **256 bits** of entropy at least equal to the greatest security strength, according to NIST SP 800-57, of the keys and hashes that it will generate.

6.1.3 Identification and authentication (FIA)

6.1.3.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when **the Number for the specified Sign In method in Table 13 of** unsuccessful authentication attempts occur related to **the Event for the same Sign In method in Table 13**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall **perform the Action for the same Sign In method in Table 13**.

Application Note: *Multiple unsuccessful authentication attempts using the same authentication data are counted as just one unsuccessful authentication attempt by the sign-in methods. For example, assuming the LDAP Sign In method has zero unsuccessful authentication attempts, if the same user types the same incorrect password into the LDAP Sign In method seven times in a row, the sign-in method will only count it as one unsuccessful authentication attempt.*

Sign In method	**Number**	**Event**	**Action**
Local Device Sign In: Device Administrator	An administrator configurable positive integer within 3 to 10	The last successful authentication for the Device Administrator within the account reset lockout counter interval	Lock account for the administrator configurable account lockout interval

Sign In method	Number	Event	Action
LDAP Sign In	6	The last successful authentication for the indicated LDAP Sign In user	Insert a 10 second delay between authentication attempts of the indicated user until: ● a successful authentication of the indicated user occurs, or ● 5 minutes elapses after the last failed authentication attempt of the indicated user.
Windows Sign In	6	The last successful authentication for the indicated Windows Sign In user	Insert a 10 second delay between authentication attempts of the indicated user until: ● a successful authentication of the indicated user occurs, or ● 5 minutes elapses after the last failed authentication attempt of the indicated user.

Table 13: Account lockout for each sign-in method

6.1.3.2 Local user attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **Control Panel users:**
  - **User identifier (display name) for Local Device Sign In only**
  - **Administrator Access Code for Local Device Sign In only**
  - **User role (defined by session permission set) for both local and remote sign-in methods**
- **IPsec users:**
  - **User identifier (defined by IP address)**
  - **User role (defined by IPsec/Firewall service template).**

Application Note:

The LDAP and Windows Sign In methods' security attributes (i.e., username, password, and groups) belonging to individual users are not in FIA_ATD.1 because these attributes are "maintained" independently by the LDAP server and Windows domain controller, respectively, which are part of the Operational Environment.

6.1.3.3 Timing of Control Panel authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow

- **Viewing of help information**
- **Viewing of device status information**
- **Viewing of network connectivity status information**
- **Viewing of system time (MFP only)**
- **Viewing of Web Services status information**
- **Viewing of Welcome screen**

- **Selection of Sign In**
- **Selection of sign-in method from Sign In screen**
- **Selection of an application**
- **Printing of help information**
- **Printing of network connectivity status information**
- **Changing language for the session**
- **Resetting of session**

on behalf of the *Control Panel* user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each *Control Panel* user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.4 IPsec authentication before any action (FIA_UAU.2)

FIA_UAU.2.1 The TSF shall require each *computer and trusted IT product connection* ~~user~~ to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that *connection* ~~user~~.

6.1.3.5 Control Panel protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only **asterisk or dot characters—depending on the HCD model—for each**

- **Administrator Access Code character entered**
- **Authentication password character entered**

to the user while the *Control Panel* authentication is in progress.

6.1.3.6 Timing of Control Panel identification (FIA_UID.1)

FIA_UID.1.1 The TSF shall allow

- **Viewing of help information**
- **Viewing of device status information**
- **Viewing of network connectivity status information**
- **Viewing of system time (MFP only)**
- **Viewing of Web Services status information**
- **Viewing of Welcome screen**
- **Selection of Sign In**
- **Selection of sign-in method from Sign In screen**
- **Selection of an application**
- **Printing of help information**
- **Printing of network connectivity status information**
- **Changing language for the session**
- **Resetting of session**

on behalf of the *Control Panel* user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each *Control Panel* user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.3.7 IPsec identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each *Administrative Computer and trusted IT product connection* ~~user~~ to be successfully identified before allowing any other TSF-mediated actions on behalf of that *connection* ~~user~~.

6.1.3.8 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user:

1. **User identifier:**
   - **Display name for Local Device Sign In**
   - **Username for remote sign-in**
   - **IP address for IPsec**
2. **User role:**
   - **User session permissions for Control Panel users**
   - **Administrator role for IPsec users.**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on behalf of users:

Control Panel user session permissions:

- **Local Device Sign In:**
  - **Device Administrator session permissions = Device Administrator permission set (PS)**
- **Remote sign-in (LDAP Sign In and Windows Sign In):**
  - **If a permission set is associated with a network user account, then:**
    User session permissions = Network user PS + Device Guest PS
  - **else, if the network user is associated with one or more network group permission sets, then:**
    User session permissions = Network group PSes + Device Guest PS
  - **else:**
    User session permissions = Remote sign-in method PS + Device Guest PS
- **If "Allow users to choose alternate sign-in methods at the product control panel" is disabled, the user's session permissions calculated above will be reduced to exclude the permissions of applications whose sign-in method does not match the sign-in method used by the user to sign in.**

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with the subjects acting on the behalf of users:

- **None—The TOE does not allow a subject to change its in-session security attributes.**

6.1.4 Security management (FMT)

6.1.4.1 Management of authentication behavior (FMT_MOF.1-auth)

FMT_MOF.1.1 The TSF shall restrict the ability to **enable, disable** the functions **"Allow users to choose alternate sign-in methods at the product control panel" for Control Panel applications** to **administrator**.

6.1.4.2 Management of authentication behavior (FMT_MOF.1-lockout)

FMT_MOF.1.1 The TSF shall restrict the ability to **enable, disable, determine the behaviour of, modify the behaviour of** the functions **account lockout policy for the Device Administrator account** to **administrator**.

6.1.4.3 Management of IPsec TSF data (FMT_MTD.1-ipsec)

Operations	TSF data	Authorized identified roles
Add, replace, delete	IPsec CA X.509v3 certificate	Administrator
Replace	IPsec identity X.509v3 certificate	
Create, modify, delete	IPsec/Firewall address templates and rules for IPsec users	
Create, modify, delete	IPsec/Firewall address templates, service templates, and rules for trusted IT products	

Table 14: IPsec TSF data management

FMT_MTD.1.1 The TSF shall restrict the ability to **perform the operations defined in Table 14 on** the **TSF data defined in Table 14** to **the authorized identified roles defined in Table 14**.

6.1.4.4 Management of miscellaneous TSF data (FMT_MTD.1-misc)

Operations	TSF data	Authorized identified roles
Modify	Administrator Access Code	Administrator
Modify	Sign-in method-to-application associations	
Modify	System time	

Table 15: Miscellaneous TSF data management

FMT_MTD.1.1 The TSF shall restrict the ability to **perform the operations defined in Table 15 on** the **TSF data defined in Table 15** to **the authorized identified roles defined in Table 15**.

6.1.4.5 Management of permission sets (FMT_MTD.1-permset)

Operations	TSF data	Authorized identified roles
Create, modify, delete	Custom permission sets	Administrator
Modify	Permissions in the Device User permission set	
	Permission set associated with each remote sign-in method	
Set, modify, delete	Permission set associated with each network user account	
	Permission set associated with each network group	

Table 16: Permission set management

FMT_MTD.1.1 The TSF shall restrict the ability to **perform the operations defined in Table 16 on** the **TSF data defined in Table 16** to **the authorized identified roles defined in Table 16**.

6.1.4.6 Specification of management functions (FMT_SMF.1)

Management functions	Matching SFR
Administrator Access Code management	FMT_MTD.1-misc
IPsec certificate management	FMT_MTD.1-ipsec
IPsec/Firewall management	
Sign In policy management	FMT_MOF.1-auth
System time management	FMT_MTD.1-misc

Table 17: TOE management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **see Table 17**.

6.1.4.7 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **administrator**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.1.5.2 Intrusion detection and response for XIP code (FPT_XCP_EXT.1)

FPT_XCP_EXT.1.1 The TSF shall perform continuous, run-time, cryptographic integrity checks of XIP code to detect potential intrusions.

FPT_XCP_EXT.1.2 The TSF shall attempt to provide the following notifications upon detection of a potential intrusion:

- **Generate and forward an audit record to the syslog server (if a syslog server is configured),**
- **Create an entry in the event log stored in the TOE, and**
- **Display an error message on the Control Panel.**

FPT_XCP_EXT.1.3 The TSF shall attempt to provide the following actions upon detection of a potential intrusion:

- **Take device offline,**
- **Initiate a reboot of the TOE, and**
- **Upon restart of the system and depending on an administrator configurable auto-recovery option, either halt the boot process in the BIOS awaiting human confirmation or continue into a full reboot of the TOE.**

6.1.6 TOE access (FTA)

6.1.6.1 Control Panel TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate ~~an~~ *a Control Panel* interactive session after ~~a~~ **20 seconds of user inactivity**.

6.1.7 Trusted path/channels (FTP)

6.1.7.1 Inter-TSF trusted channel (FTP_ITC.1)

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF, another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communication over the network interface**.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security functional requirements	Objectives
FAU_GEN.1	O.AUDIT.LOGGED
FAU_GEN.2	O.AUDIT.LOGGED
FCS_CKM.1	O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FCS_CKM.2	O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FCS_COP.1-ipsec	O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FCS_COP.1-xcp	O.XIP.CHECKS
FCS_RBG_EXT.1	O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FIA_AFL.1	O.ADMIN.AUTHORIZED
FIA_ATD.1	O.ADMIN.AUTHORIZED
FIA_UAU.1	O.ADMIN.AUTHORIZED, O.INTERFACE.MANAGED
FIA_UAU.2	O.ADMIN.AUTHORIZED, O.INTERFACE.MANAGED
FIA_UAU.7	O.TSF_DATA.IN_TOE_DIS, O.TSF_DATA.IN_TOE_MOD, O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FIA_UID.1	O.ADMIN.AUTHORIZED, O.AUDIT.LOGGED, O.INTERFACE.MANAGED, O.TSF_DATA.IN_TOE_DIS, O.TSF_DATA.IN_TOE_MOD, O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FIA_UID.2	O.ADMIN.AUTHORIZED, O.AUDIT.LOGGED, O.INTERFACE.MANAGED, O.TSF_DATA.IN_TOE_DIS, O.TSF_DATA.IN_TOE_MOD, O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FIA_USB.1	O.ADMIN.AUTHORIZED
FMT_MOF.1-auth	O.TSF_DATA.IN_TOE_MOD, O.TSF_DATA.IN_TRANSIT_MOD
FMT_MOF.1-lockout	O.TSF_DATA.IN_TOE_MOD

Security functional requirements	Objectives
FMT_MTD.1-ipsec	O.TSF_DATA.IN_TOE_DIS, O.TSF_DATA.IN_TOE_MOD, O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FMT_MTD.1-misc	O.TSF_DATA.IN_TOE_DIS, O.TSF_DATA.IN_TOE_MOD, O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FMT_MTD.1-permset	O.TSF_DATA.IN_TOE_DIS, O.TSF_DATA.IN_TOE_MOD
FMT_SMF.1	O.TSF_DATA.IN_TOE_DIS, O.TSF_DATA.IN_TOE_MOD, O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FMT_SMR.1	O.ADMIN.AUTHORIZED, O.TSF_DATA.IN_TOE_DIS, O.TSF_DATA.IN_TOE_MOD, O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD
FPT_STM.1	O.AUDIT.LOGGED
FPT_XCP_EXT.1	O.XIP.CHECKS, O.XIP.RESPONSE
FTA_SSL.3	O.ADMIN.AUTHORIZED, O.INTERFACE.MANAGED
FTP_ITC.1	O.TSF_DATA.IN_TRANSIT_DIS, O.TSF_DATA.IN_TRANSIT_MOD

Table 18: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security objectives	Rationale
O.ADMIN.AUTHORIZED	The objective: ● The TOE shall require identification and authentication of administrators, and shall ensure that administrators are authorized in accordance with security policies before allowing them to use the TOE. is met by:

Security objectives	Rationale
	● FIA_AFL.1 which slows the number of unsuccessful Control Panel authentication attempts made over a period of time. ● FIA_ATD.1 which supports authorization by associating security attributes with users. ● FIA_UAU.1 and FIA_UAU.2 which enforce authorization by requiring user authentication. ● FIA_UID.1 and FIA_UID.2 which enforce authorization by requiring user identification. ● FIA_USB.1 which enforces authorization by distinguishing subject security attributes associated with user roles. ● FMT_SMR.1 which supports authorization by requiring security roles. ● FTA_SSL.3 which enforces authorization by terminating inactive sessions.
O.AUDIT.LOGGED	The objective: ● The TOE shall generate audit data of TOE use and security-relevant events. is met by: ● FAU_GEN.1 which enforces audit policies by requiring logging of relevant events. ● FAU_GEN.2 which enforces audit policies by requiring logging of user identity information associated with audited events caused by a user. ● FIA_UID.1 and FIA_UID.2 which support audit policies by requiring the TOE to identify TOE users, thus, allowing for the association of user identity with events ● FPT_STM.1 which supports audit policies by requiring reliable time stamps and allowing these time stamps to be associated with audit events.
O.INTERFACE.MANAGED	The objective: ● The TOE shall manage the operation of external interfaces in accordance with security policies. is met by: ● FIA_UAU.1 and FIA_UAU.2 which enforce management of external interfaces by requiring user authentication. ● FIA_UID.1 and FIA_UID.2 which enforce management of external interfaces by requiring user identification. ● FTA_SSL.3 which enforces management of external interfaces by terminating inactive sessions.
O.TSF_DATA.IN_TOE_DIS	The objective: ● The TOE shall protect TSF data in the TOE from unauthorized disclosure. is met by:

Security objectives	Rationale
	● FIA_UID.1 and FIA_UID.2 which support security roles by requiring user identification. ● FMT_MTD.1-ipsec, FMT_MTD.1-misc, and FMT_MTD.1-permset which enforce protection of TSF data by restricting access. ● FMT_SMF.1 which supports control of security attributes and TSF data by requiring functions to control attributes. ● FMT_SMR.1 which supports control of security attributes and TSF data by requiring security roles.
O.TSF_DATA.IN_TOE_MOD	The objective: ● The TOE shall protect TSF data in the TOE from unauthorized modification. is met by: ● FIA_UID.1 and FIA_UID.2 which support security roles by requiring user identification. ● FMT_MOF.1-auth which specifies the roles that can manage the selection of sign-in methods. ● FMT_MOF.1-lockout which specifies the Control Panel lockout policy for the local Device Administrator account. ● FMT_MTD.1-ipsec, FMT_MTD.1-misc, and FMT_MTD.1-permset which enforce protection of TSF data by restricting access. ● FMT_SMF.1 which supports control of security attributes and TSF data by requiring functions to control attributes. ● FMT_SMR.1 which supports control of security attributes and TSF data by requiring security roles.
O.TSF_DATA.IN_TRANSIT_DIS	The objective: ● The TOE shall protect TSF data on the network from unauthorized disclosure. is met by: ● FCS_CKM.1 which specifies the type of cryptographic keys generated for IPsec key establishment. ● FCS_CKM.2 which specifies the cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec to create a channel protected from unauthorized disclosure. ● FCS_COP.1-ipsec which specifies the RSA signature generation and verification along with the AES and HMAC cryptographic algorithms used by IPsec to help prevent unauthorized disclosure. ● FCS_RBG_EXT.1 which specifies the random bit generation used by IPsec. ● FIA_UAU.7 which masks the display of certain passwords during authentication. ● FIA_UID.1 and FIA_UID.2 which support security roles by requiring user identification. ● FMT_MTD.1-ipsec and FMT_MTD.1-misc which enforce protection of TSF data by restricting access.

Security objectives	Rationale
	● FMT_SMF.1 which supports control of security attributes by requiring functions to control attributes. ● FMT_SMR.1 which supports control of security attributes by requiring security roles. ● FTP_ITC.1 which enforces protection by requiring the use of trusted channels for communication of data over network Interfaces.
O.TSF_DATA.IN_TRANSIT_MOD	The objective: ● The TOE shall protect TSF data on the network from unauthorized modification. is met by: ● FCS_CKM.1 which specifies the type of cryptographic keys generated for IPsec key establishment. ● FCS_CKM.2 which specifies the cryptographic key establishment methods used by IKEv1 and IKEv2 in IPsec to create a channel that detects unauthorized modification. ● FCS_COP.1-ipsec which specifies the SHA and HMAC cryptographic algorithms used by IPsec to detect unauthorized modification. ● FCS_RBG_EXT.1 which specifies the random bit generation used by IPsec. ● FIA_UAU.7 which masks the display of certain passwords during authentication. ● FIA_UID.1 and FIA_UID.2 which support security roles by requiring user identification. ● FMT_MOF.1-auth which specifies the roles that can manage the selection of sign-in methods. ● FMT_MTD.1-ipsec and FMT_MTD.1-misc which enforce protection of TSF data by restricting access. ● FMT_SMF.1 which supports control of security attributes and TSF data by requiring functions to control attributes. ● FMT_SMR.1 which supports control of security attributes by requiring security roles. ● FTP_ITC.1 which enforces protection by requiring the use of trusted channels for communication of data over network Interfaces.
O.XIP.CHECKS	The objective: ● The TOE shall perform continuous, run-time, cryptographic integrity checks of XIP code to detect potential intrusions. is met by: ● FCS_COP.1-xcp which specifies the message digest used to perform the XIP integrity checks. ● FPT_XCP_EXT.1 which specifies the cryptographic integrity checking of the XIP code during runtime.
O.XIP.RESPONSE	The objective:

Security objectives	Rationale
	● If an integrity check of XIP code fails, the TOE shall notify of and recover from the potential intrusion. is met by: ● FPT_XCP_EXT.1 which specifies responses/actions to integrity check inconsistencies found by the cryptographic checking of the XIP code during runtime.

Table 19: Security objectives for the TOE rationale

6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of the SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1	FAU_GEN.1
	FIA_UID.1	FIA_UID.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_CKM.2 FCS_COP.1-ipsec
	FCS_CKM.4	This dependency is unresolved. The generated keys are not formally destroyed. The object reuse mechanisms of the operating system prevent their use except in the intended context.
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The generated keys are not formally destroyed. The object reuse mechanisms in the operating system prevent their use except in the intended context.
FCS_COP.1-ipsec	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The keys used for encryption, decryption, and data authentication are not formally destroyed. The object reuse mechanisms in the operating system prevent their use except in the intended context.

Security functional requirement	Dependencies	Resolution
FCS_COP.1-xcp	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is unresolved. There are no keys generated for or used by this hash algorithm.
	FCS_CKM.4	This dependency is unresolved. There are no keys used by this hash algorithm, thus, there are no keys to destroy.
FCS_RBG_EXT.1	No dependencies	
FIA_AFL.1	FIA_UAU.1	FIA_UAU.1
FIA_ATD.1	No dependencies	
FIA_UAU.1	FIA_UID.1	FIA_UID.1
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.1	No dependencies	
FIA_UID.2	No dependencies	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1-auth	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MOF.1-lockout	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1-ipsec	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1-misc	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1-permset	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_SMF.1	No dependencies	
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FPT_STM.1	No dependencies	
FPT_XCP_EXT.1	FAU_GEN.1	FAU_GEN.1
FTA_SSL.3	No dependencies	

Security functional requirement	Dependencies	Resolution
FTP_ITC.1	No dependencies	

Table 20: TOE SFR dependency analysis

6.2.4 Internal consistency and mutual support of SFRs

6.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are the Evaluation Assurance Level 2 components as specified in [CC] part 3, augmented by ALC_FLR.2.

The following table shows the SARs, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	**Ref.**	**Ass.**	**Sel.**
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.2 Security-enforcing functional specification	CC Part 3	No	No	No	No
	ADV_TDS.1 Basic design	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.2 Use of a CM system	CC Part 3	No	No	No	No
	ALC_CMS.2 Parts of the TOE CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No
	ALC_FLR.2 Flaw reporting procedures	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.1 Evidence of coverage	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ATE_FUN.1 Functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.2 Vulnerability analysis	CC Part 3	No	No	No	No

Table 21: SARs

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen to match a Basic attack potential, commensurate with the threat environment that is experienced by typical consumers of the TOE. In addition, the evaluation assurance level has been augmented with ALC_FLR.2, commensurate with the augmented flaw remediation capabilities offered by the developer beyond those required by the evaluation assurance level.

7 TOE Summary Specification

7.1 TOE Security Functionality

The following section explains how the security functions are implemented by the TOE. The different TOE security functions cover the various SFR classes.

The primary security features of the TOE are:

- Auditing,
- Cryptography,
- Identification and authentication,
- Protection of the TSF,
- TOE access protection,
- Trusted channel communication and certificate management, and
- Security management.

7.1.1 Auditing

The TOE performs auditing of security relevant functions. The TOE connects and sends audit records to a syslog server (part of the Operational Environment) for long-term storage and audit review. The records sent to the syslog server by the TOE are only those generated by the TOE while the syslog server has an established connection with the TOE. If the connection between the TOE and syslog server breaks and is later reestablished, only records generated by the TOE after the connection is reestablished are sent to the syslog server. Both the Jetdirect Inside Firmware and System Firmware generate audit records.

The types of records generated by the TOE are specified in section 6.1.1.1. Each record includes the date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. Events resulting from actions of identified users are associated with the identity of the user that caused the event.

The subject identity used in the audit record is formed in the following manner. For Local Device Sign In, the subject's identity contains the user's Display Name prefixed with "LOCAL\". For LDAP Sign In, the subject's identity contains the user's LDAP user name prefixed with either the LDAP server's host name or IP address then a backslash. For Windows Sign In, the subject's identity contains the user's Windows domain name and Windows user name separated by a "\". For IPsec, the subject's identity is the user's IP address.

The time source used for the audit record timestamps is discussed in section 7.1.4.2.

This section maps to the following SFRs.

- FAU_GEN.1
- FAU_GEN.2

7.1.2 Cryptography

The TOE uses IPsec to protect its communications channels. The QuickSec cryptographic library, which is part of the Operational Environment, is used to supply the cryptographic algorithms for IPsec. See section 7.1.6 for more information.

The TOE's XIP code protection functionality uses the MD5 message digest algorithm to perform integrity checks on the XIP code. This algorithm is inside the TOE boundary. See section 7.1.4.1 for more information.

7.1.3 Identification and authentication (I&A)

The TOE supports multiple Control Panel sign-in methods, both local and remote methods. It also supports IPsec identification and mutual authentication.

The following interfaces support I&A.

- Control Panel
- IPsec

The following interface allows a user limited TOE access without I&A.

- Analog Fax Phone Line (for incoming analog fax phone line users)

7.1.3.1 Control Panel I&A

The HCD has a Control Panel used to identify and authenticate users as well as to select a function (a.k.a. Control Panel application) to be performed. The Control Panel supports both local and remote sign-in methods (a.k.a. internal and external authentication mechanisms).

The local sign-in method, which is part of the TOE firmware, supported in the evaluated configuration is:

- Local Device Sign In

The remote sign-in methods, which are part of the Operational Environment, supported in the evaluated configuration are:

- LDAP Sign In
- Windows Sign In (via Kerberos)

Although the Local Device Sign In method supports multiple accounts, only the built-in Device Administrator account is to be used with this method in the evaluated configuration. The administrator must not create any Local Device Sign In accounts (a.k.a. User Access Codes).

The built-in Device Administrator account contains a display name (admin) used as an identifier and an Administrator Access Code used as the authenticator. The Administrator Access Code can be up to 16 characters in length, composed of letters, numbers, and special characters, and can be modified by an administrator.

The remote sign-in methods both use a username and password as the user account's identifier and authenticator, respectively. Each remote sign-in method determines the username and password character composition characteristics.

Control Panel user roles are determined by permission sets. The Control Panel uses permissions to determine which Control Panel applications a user can access. Each Control Panel application requires one or more permissions in order to execute it. Each Control Panel user has one or more permission sets associated with their account. The user's combined permission sets determines the user's role when logged in.

For all Control Panel account types, the permission set (PS) data are stored in the TOE and managed via EWS and WS* Web Services. The default administrative permission set in the evaluated configuration is the Device Administrator PS.

The built-in Device Administrator account has the Device Administrator PS permanently assigned to it. Summing up, the Device Administrator account has the following security attributes that are maintained by the TOE.

- Display name (admin)
- Administrator Access Code (up to 16 characters)
- Permission set (permanently set to Device Administrator PS)

For successful local I&A, the user must select the Device Administrator account (i.e., Administrator Access Code access type) and correctly enter the Device Administrator password.

Each remote sign-in account (a.k.a. network user account) contains the following security attributes.

- Username (maintained by the Operational Environment)
- Password (maintained by the Operational Environment)
- Groups (maintained by the Operational Environment)
- Permission set (maintained by the TOE)

For successful remote I&A, the user must enter a valid username and password as defined by the remote sign-in method. Limitations on the username and password compositions are enforced by the remote sign-in method, not the TOE. Though the username and password are maintained by the remote sign-in method, the permission set is maintained locally by the TOE.

For remote sign-in methods, the TOE receives the authentication credentials from the Control Panel users and passes the credentials to the remote sign-in method. The remote sign-in method returns an authentication decision to the TOE. This decision is then enforced by the TOE by granting or denying access to the Control Panel user.

In the case of LDAP, the username and password entered at the Control Panel are used to bind to the LDAP server. The user must have a valid and active LDAP account in order to successfully bind using this method.

In the case of Kerberos, the username and password entered at the Control Panel are used to authenticate with the Windows domain controller. The user must have a valid and active Windows domain account in order to successfully use this method.

When a user successfully logs in to the Control Panel, the permission set (a.k.a. session permission set) associated with that user is calculated and bound to that user-instance and defines the user's role.

When a user signs in through the Control Panel, the TOE displays either asterisks or dots—depending on the HCD model—for each character entered of the Administrator Access Code and remote sign-in password to prevent onlookers from viewing another user's authentication data.

Prior to signing in, the Control Panel allows users to perform the following functions.

- Viewing of help information
- Viewing of device status information
- Viewing of network connectivity status information
- Viewing of system time (MFP only)
- Viewing of Web Services status information
- Viewing of Welcome screen
- Selection of Sign In
- Selection of sign-in method from Sign In screen

- Selection of an application
- Printing of help information
- Printing of network connectivity status information
- Changing language for the session
- Resetting of session

This section maps to the following SFRs.

- FIA_ATD.1
- FIA_UAU.1
- FIA_UAU.7
- FIA_UID.1
- FIA_USB.1
- FMT_SMR.1

7.1.3.1.1 Permission sets

Permission sets are used to determine which Control Panel applications a Control Panel user can access. A permission set contains a list of allowed permissions.

The TOE contains the following built-in permission sets.

- Device Administrator—Grants administrative capabilities
- Device User—Grants typical user capabilities
- Device Guest—Grants capabilities to non-logged on users

These built-in permission sets cannot be renamed or deleted. The Device Administrator and Device Guest permission sets cannot be modified, but an administrator can modify the permissions in the Device User permission set. In the evaluated configuration, the Device Guest permission set is empty (i.e., contains no permissions).

As an alternative to built-in permission sets, administrators can create custom permission sets that allow an administrator to better map the TOE's permissions to the usage model of their organization. Administrators can also modify and delete any existing custom permission sets. By default, the TOE comes with no custom permission sets.

All permission sets are stored and maintained locally on the TOE for both local device user accounts and network user accounts (including network group and remote sign-in method permission sets).

This section maps to the following SFRs.

- FIA_USB.1
- FMT_MTD.1-permset
- FMT_SMR.1

7.1.3.1.1.1 Local Device Sign In method session permission set

For the Local Device Sign In method, the evaluated configuration only supports the local Device Administrator account. This account has the Device Administrator PS permanently assigned to it; thus, its session permission set is always equal to the Device Administrator PS.

This section maps to the following SFRs.

- FIA_USB.1

- FMT_SMR.1

7.1.3.1.1.2 Remote sign-in method session permission set

Network user accounts introduce the concept of network groups. A network group (a.k.a. group) is a collection of zero or more network user accounts. Each remote sign-in method defines its own groups. The members of a group are comprised of the network user accounts from that remote sign-in method. A network user account can be associated with zero or more groups.

A TOE administrator can associate zero or one permission set to each group and zero or one permission set to each network user account. These associations are maintained and stored on the TOE. A TOE administrator can create, modify, and delete these associations. By default, there are no permission set associations for network user accounts and groups.

A permission set is associated with each remote sign-in method. These associations are also maintained and stored on the TOE. A TOE administrator can modify these associations.

The TOE combines these various permission sets in one of the following three ways.

If the network user account has a permission set association, then the TOE combines the network user account's permission set and the Device Guest permission set to create the network user’s session permission set.

```
User session permissions = Network user account PS + Device Guest PS
```

If the network user account does not have an associated permission set, the TOE obtains the groups to which the network user account is a member. For each of these groups, the TOE looks for matching group to permission set associations. For each group to permission set association match, the TOE combines that group’s permissions with any previously found group permissions. Once all matches have been found, the TOE combines these group permissions with the Device Guest permission set to create the network user's session permission set.

```
User session permissions = Network group PSes + Device Guest PS
```

If there are no group to permission set associations found for the network user account and the network user account does not have an associated permission set, then the TOE combines the remote sign-in method's permission set and the Device Guest permission set to create the network user’s session permission set.

```
User session permissions = Remote sign-in method PS + Device Guest PS
```

This section maps to the following SFRs.

- FIA_USB.1
- FMT_MTD.1-permset
- FMT_SMR.1

7.1.3.1.2 Account Lockout

The Control Panel contains two account lockout mechanisms. One mechanism is used for the local Device Administrator account. The other mechanism, called Simplified Account Lockout, is used for all other Control Panel account types.

Device Administrator Account Lockout

For the Device Administrator account, the Control Panel's lockout mechanism uses the following control values.

- Account lockout maximum attempts

- Account lockout interval
- Account reset lockout counter interval

The *account lockout maximum attempts* value allows an administrator to control the number of failed authentication attempts on the account before it is locked. The administrator can choose a value between 3 and 10 inclusively. Consecutive failed authentication attempts using the same authentication credential count as a single failed authentication attempt. The counted failed attempts must happen within the value set for the *account reset lockout counter interval*; otherwise, the maximum attempts counter is reset when the *account reset lockout counter interval* value elapses. The *account lockout interval* value defines the duration of the lockout.

Simplified Account Lockout

For all other Control Panel account types, the Control Panel interface contains a feature called Simplified Account Lockout to help protect against brute-force attacks at the Control Panel. Each Control Panel sign-in method performs its Simplified Account Lockout independent of the other Control Panel sign-in methods.

The LDAP Sign In method inserts a 10 second delay between each authentication attempt by the same LDAP user upon reaching 6 failed attempts. It keeps inserting the delay until either:

- the indicated LDAP user successfully authenticates, or
- 5 minutes elapses after the last failed authentication attempt by the indicated LDAP user.

Like the LDAP Sign In method, the Windows Sign In method inserts a 10 second delay between each authentication attempt by the same Windows user upon reaching 6 failed attempts. It keeps inserting the delay until either:

- the indicated Windows user successfully authenticates, or
- 5 minutes elapses after the last failed authentication attempt by the indicated Windows user.

Multiple unsuccessful authentication attempts using the same authentication data are counted as just one unsuccessful authentication attempt by the sign-in methods. For example, assuming the LDAP Sign In method has zero unsuccessful authentication attempts, if the same user types the same incorrect password into the LDAP Sign In method seven times in a row, the sign-in method will only count it as one unsuccessful authentication attempt.

This section maps to the following SFR.

- FIA_AFL.1
- FMT_MOF.1-lockout

7.1.3.2 IPsec I&A

The TOE uses IPsec to identify and mutually authenticate the following user type.

- Administrative Computer

IPsec uses IP addresses and RSA X.509v3 certificates via the IKE protocols (IKEv1 and IKEv2) to identify and authenticate a client computer. The TOE contains one X.509v3 identity certificate and one or more X.509v3 CA certificates to use for the IPsec mutual authentication. The TOE does not maintain individual X.509v3 certificates of its client computers.

The User Identity of a client computer is its IP address. The TOE's internal firewall maintains lists (IPsec/Firewall address templates) of IP addresses of client computers that can connect to the TOE. If a client computer has an unrecognized IP address that is not defined in the IPsec/Firewall, then the client computer is not allowed to connect to the TOE. Similarly, if the client computer presents an invalid or unknown (unrecognized CA) X.509v3 certificate, the IPsec mutual authentication mechanism will fail. The TOE uses RSA signature generation and signature verification methods as part of this validity checking process.

The TOE also uses IP addresses and X.509v3 certificates via the IKE protocols to connect to and identify other trusted IT products. See section 7.1.6 for more details.

The TOE supports the following versions of the IKE protocol.

- IKEv1 ([RFC4109])
- IKEv2 ([RFC4306] and [RFC4718])

Mutual identification and authentication must be completed before any tasks can be performed by a client computer.

The service templates define the user role of a client computer. The following service template is used to define the Administrator Computer for IPsec users.

- All Services

The All Services service template is provided with the TOE.

The Administrative Computer can access the PJL Interface on port 9100 as well as the EWS (HTTP) interface, Web Services interface (OXPd and WS*), and SNMP interface.

The TOE uses the IPsec/Firewall to control access to the supported network service protocols. The IPsec/Firewall contains the IP addresses of authorized client computers grouped into address templates and the network service protocols grouped into service templates. The administrator maps an address template to a service template using an IPsec/Firewall rule. Service templates, therefore, act as the user roles for IPsec users. IP addresses of computers not contained in a rule are denied access to the TOE.

This section maps to the following SFRs.

- FIA_ATD.1
- FIA_UAU.2
- FIA_UID.2
- FIA_USB.1
- FMT_SMR.1

7.1.4 Protection of the TSF

7.1.4.1 Intrusion detection

Once the TOE is instantiated, the TOE runs continuous, cryptographic integrity checks on XIP code using the MD5 message digest. Failing one or more of these integrity checks may indicate a possible tampering of the code, thus, it may indicate an intrusion or an attack by someone attempting to violate the TOE's security policy. If the TOE detects an intrusion by the failure of one or more of these integrity checks, the TOE will attempt to perform the following notifications.

- Generate and forward an audit record to the syslog server (if a syslog server is configured)
- Create an entry in the event log stored in the TOE
- Display an error message on the Control Panel

In addition, the TOE will attempt to perform the following actions.

- Take device offline
- Initiate a reboot of the TOE

- Upon restart of the system and depending on an administrator configurable auto-recovery option, either halt the boot process in the BIOS awaiting human confirmation or continue into a full reboot of the TOE. (The auto-recovery option is configured once during the initial setup of the evaluated configuration.)

Depending on the extent of the intrusion, the TOE may or may not be able to perform one or more of these notifications and actions. If the device is able to restart, an administrator can configure the HCD to either halt the boot process in the BIOS awaiting human confirmation or continue into a full reboot of the TOE.

This section maps to the following SFRs.

- FCS_COP.1-xcp
- FMT_SMF.1
- FPT_XCP_EXT.1

7.1.4.2 Reliable timestamps

The TOE contains a system clock that is used to generate reliable timestamps. Only an administrator can manage the system clock.

This section maps to the following SFR.

- FPT_STM.1

7.1.5 TOE access protection

7.1.5.1 Inactivity timeout

The TOE supports an inactivity timeout for Control Panel sessions. If a logged in user is inactive for longer than the specified period, the user is automatically logged off of the TOE. The inactivity period is managed by the administrator via EWS (HTTP), WS* web services, or the Control Panel. A single inactivity period setting exists per TOE.

This section maps to the following SFR.

- FTA_SSL.3

7.1.6 Trusted channel communication and certificate management

Network communications (i.e., Ethernet) between the TOE and other trusted IT products use a trusted channel mechanism to protect the communications from disclosure and modification. The TOE also ensures the cryptographic operations are validated during policy processing such as validating digital signatures or encrypting and decrypting data. The following table provides a list of the mechanism(s) used to protect these channels and the channels protected by the mechanism(s).

Secure protocol	Network channel	HCD type	Initiated by
IPsec	Email connections (SMTP gateway)	SFP, MFP	TOE
	EWS (HTTP) connections (including web browser & certificate upload)	SFP, MFP	Administrative Computer

Secure protocol	Network channel	HCD type	Initiated by
	Windows domain controller (Kerberos) connections	SFP, MFP	TOE
	LDAP server connections	SFP, MFP	TOE
	PJL connections	SFP, MFP	Administrative Computer & Client computers
	Save to Network Folder connections (SMB, FTP)	MFP	TOE
	Save to SharePoint connections (*flow* models only)	MFP	TOE
	SNMP connections	SFP, MFP	Administrative Computer
	Syslog server connections	SFP, MFP	TOE
	Web Services connections (OXPd & WS*)	SFP, MFP	Administrative Computer

Table 22: Trusted channel connections

As shown in Table 22, the Save to Network Folder and Save to SharePoint features are not supported by the SFPs.

The TOE uses IPsec as means to provide trusted channel communications. IPsec uses X.509v3 certificates, the Encapsulating Security Payload (ESP), Internet Security Association and Key Management Protocol (ISAKMP), IKEv1, and IKEv2 protocols, and the cryptographic algorithms listed below to protect communications.

The cryptographic functions used by IPsec are implemented in the QuickSec cryptographic library version 5.1 ([QuickSec51]) which is produced by INSIDE Secure. The QuickSec cryptographic library is part of the Operational Environment, not the TOE. The TOE prepares the data and invokes the appropriate cryptographic functions, but the code in the QuickSec cryptographic library performs the processing and calculations required. INSIDE Secure performs regular and rigorous developer testing of the implementation of the cryptographic algorithms in the QuickSec cryptographic library.

In the evaluated configuration, the following IPsec cryptographic algorithms are supported.

- DH (IKEv1, IKEv2) key establishment/exchange (Operational Environment)
- DSA 2048-bit key pair generation (Operational Environment)
- RSA 2048-bit and 3072-bit signature generation and verification (Operational Environment)
- AES-128, AES-192, and AES-256 in CBC mode for data transfers (Operational Environment)
- AES-256 (with ECB mode) for the CTR_DRBG(AES) (Operational Environment)
- CTR_DRBG(AES) (Operational Environment)
- SHA-1, SHA-256, SHA-384, and SHA-512 hashing (Operational Environment)
- HMAC-SHA1-96 (Operational Environment)
- HMAC-SHA-256-128 (Operational Environment)
- HMAC-SHA-384-192 (Operational Environment)
- HMAC-SHA-512-256 (Operational Environment)

IPsec is conformant to the MUST/MUST NOT requirements of the following Internet Engineering Task Force (IETF) Request for Comments (RFCs).

- [RFC4301] and [RFC4894] for IPsec
- [RFC4303] for ESP
- [RFC4306] for ISAKMP
- [RFC4109] and [RFC4894] for IKEv1
- [RFC4306], [RFC4718], and [RFC4894] for IKEv2

The TOE maintains the following X.509v3 certificates for IPsec in the certificate store.

- One network identity certificate
- One or more CA certificates

The EWS (HTTP), OXPd, and WS* interfaces allow administrators to manage these X.509v3 certificates used by IPsec.

When the TOE is first powered on, it generates a self-signed identity certificate to use for network identity. In the evaluated configuration, the use of a self-signed identity certificate generated by the TOE for network identity is not permitted. The administrator must import a CA-signed identity certificate and private key and designate this certificate for network identity usage. The TOE requires a network identity certificate to always exist; therefore, it allows the administrator to replace the network identity certificate used by IPsec.

The TOE uses a copy of the self-signed identity certificate it generates when first powered on as a CA certificate (self-signed) and comes with other CA certificates pre-installed. The administrator must obtain a CA certificate from the Operational Environment and install this certificate when setting up the evaluated configuration. The TOE allows the administrator to add, replace, and delete CA certificates used by IPsec.

This section maps to the following SFRs.

- FCS_CKM.1
- FCS_CKM.2
- FCS_COP.1-ipsec
- FCS_RBG_EXT.1
- FMT_MTD.1-ipsec
- FMT_SMF.1
- FTP_ITC.1

7.1.7 Security management

The TOE supports the following role.

- Administrators

Administrators maintain and configure the TOE and Operational Environment.

In addition, the TOE performs many security management functions.

Only administrators can configure the Administrative Computer that is allowed to connect to the TOE and the list of other trusted IT products to which the TOE will connect. Administrators do this by creating, modifying, and deleting IPsec/Firewall address templates, service templates, and rules via the TOE. Similarly, only administrators can create, modify, and delete address templates, service templates, and rules via the TOE for trusted IT products.

For each Control Panel application, an administrator can modify the association of a sign-in method to an application. (For example, the administrator can associate the LDAP Sign In method to the "Print from Job Storage" application). In addition, administrators control whether or not a Control Panel user must use the administrator-selected sign-in method associated with the applications in order to access that application. This latter feature is controlled through the "Allow users to choose alternate sign-in methods at the product control panel" function.

Administrators can manage the account lockout features of the Device Administrator account. Administrators can also modify the system time.

This section maps to the following SFRs.

- FMT_MOF.1-auth
- FMT_MOF.1-lockout
- FMT_MTD.1-ipsec
- FMT_MTD.1-misc
- FMT_SMF.1
- FMT_SMR.1

8 Abbreviations, Terminology and References

8.1 Abbreviations

AES
Advanced Encryption Standard

AH
Authentication Header (IPsec)

ASCII
American Standard Code for Information Interchange

BIOS
Basic Input/Output System

CA
Certificate Authority

CAPI
Cryptographic Application Programming Interface

CBC
Cipher Block Chaining

CC
Common Criteria

CTR
Counter

CTR_DRBG
Counter DRBG

DH
Diffie-Hellman

DLL
Dynamic Link Library

DNS
Domain Name System

DRBG
Deterministic Random Bit Generator

DSS
Digital Sending Software

EAL
Evaluated Assurance Level

eMMC
embedded MMC

ESP
Encapsulating Security Payload (IPsec)

EWS
Embedded Web Server

FFC
Finite Field Cryptography

FIH
Foreign Interface Harness

FTP
File Transfer Protocol

HCD
Hardcopy Device

HMAC
Hashed Message Authentication Code

HP
Hewlett-Packard

HTML
Hypertext Markup Language

HTTP
Hypertext Transfer Protocol

IEEE
Institute of Electrical and Electronics Engineers, Inc.

IETF
Internet Engineering Task Force

IKE
Internet Key Exchange (IPsec)

IP
Internet Protocol

IPsec
Internet Protocol Security

ISAKMP
Internet Security Association Key Management Protocol (IPsec)

LCD
Liquid Crystal Display

LDAP
Lightweight Directory Access Protocol

MAC
Message Authentication Code

MD5
Message Digest 5

MFP
Multifunction Product

MMC
MultiMediaCard

NFC
Near Field Communication

NTLM
Microsoft NT LAN Manager

NTP
Network Time Protocol

OSP
Organizational Security Policy

OXP
Open Extensibility Platform

OXPd
OXP device layer

PDF
Portable Document Format

PIN
Personal Identification Number

PJL
Printer Job Language

PP
Protection Profile

PRF
Pseudo-random Function

PS
Permission Set

PS
PostScript

PSTN
Public Switched Telephone Network

RAM
Random Access Memory

RFC
Request for Comments

RJ11
Registered Jack Function 11

RJ45
Registered Jack Function 45

RSA
Rivest-Shamir-Adleman

S/MIME
Secure/Multipurpose Internet Mail Extensions

SAR
Security Assurance Requirement

SFP
Single-Function Printer

SFR
Security Functional Requirement

SHA
Secure Hash Algorithm

SMB
Server Message Block

SMTP
Simple Mail Transfer Protocol

SNMP
Simple Network Management Protocol

SOAP
Simple Object Access Protocol

SSD
Solid State Drive

SSH
Secure Shell

ST
Security Target

TOE
Target of Evaluation

TSF
TOE Security Functionality

TSP
TOE Security Policy

USB
Universal Serial Bus

WINS
Windows Internet Name Service

XIP
Execute In-Place

XML
Extensible Markup Language

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Administrative User
This term refers to a user with administrative control of the TOE.

Authentication Data
This includes the Administrator Access Code and/or password for each user of the product.

Control Panel Application
An application that resides in the firmware and is selectable by the user via the Control Panel.

Device Administrator Password
The password used to restrict access to administrative tasks via EWS, OXPd, WS*, and the Control Panel. This password is also required to associate a user with the Administrator role. In product documentation, it may also be referred to as the Local Device Administrator Password, Local Device Administrator Access Code, the Device Password, or the Administrator Password.

External Interface
A non-hardcopy interface where either the input is being received from outside the TOE or the output is delivered to a destination outside the TOE.

Hardcopy Device (HCD)
This term generically refers to the product models in this ST.

Near Field Communication (NFC)
Proximity (within a few inches) radio communication between two or more devices.

TOE Owner
A person or organizational entity responsible for protecting TOE assets and establishing related security policies.

User Security Attributes
Defined by functional requirement FIA_ATD.1, every user is associated with one or more security attributes which allow the TOE to enforce its security functions on this user.

Wireless Direct Print
Feature that enables Wi-Fi capable devices (for example: smart phones, tablets, or computers) to establish a direct peer-to-peer wireless connection with the printer to submit print jobs.

XIP Code
Code in the kernel that is built to execute from a specific location in memory, and this location cannot be changed at runtime.

8.3 References

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R5
Date April 2017
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

FIPS180-4 **Secure Hash Standard (SHS)**
Date 2015-08-04
Location https://csrc.nist.gov/publications/detail/fips/180/4/final

FIPS186-2 **Digital Signature Standard (DSS)**
Date 2001-10-05
Location https://csrc.nist.gov/CSRC/media/Publications/fips/186/2/archive/2001-10-05/documents/fips186-2-change1.pdf

FIPS197 **Advanced Encryption Standard (AES)**
Date 2001-11-26
Location https://csrc.nist.gov/publications/detail/fips/197/final

PKCS1v1.5 **Public-Key Cryptography Standard (PKCS) #1: RSA Encryption Standard**
Author(s) RSA Laboratories
Version 1.5
Date November 1993

QuickSec51 **QuickSec 5.1 Toolkit Reference Manual**
Author(s) INSIDE Secure
Version 1.0
Date December 2009

RFC1321 **The MD5 Message-Digest Algorithm**
Author(s) R. Rivest
Date 1992-04-01
Location http://www.ietf.org/rfc/rfc1321.txt

RFC2404 **The Use of HMAC-SHA-1-96 within ESP and AH**
Author(s) C. Madson, R. Glenn
Date 1998-11-01
Location http://www.ietf.org/rfc/rfc2404.txt

RFC4109 **Algorithms for Internet Key Exchange version 1 (IKEv1)**
Author(s) P. Hoffman
Date 2005-05-01
Location http://www.ietf.org/rfc/rfc4109.txt

RFC4301 **Security Architecture for the Internet Protocol**
Author(s) S. Kent, K. Seo
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4301.txt

RFC4303 **IP Encapsulating Security Payload (ESP)**
Author(s) S. Kent
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4303.txt

RFC4306 **Internet Key Exchange (IKEv2) Protocol**
Author(s) C. Kaufman
Date 2005-12-01
Location http://www.ietf.org/rfc/rfc4306.txt

RFC4718 **IKEv2 Clarifications and Implementation Guidelines**
Author(s) P. Eronen, P. Hoffman
Date 2006-10-01
Location http://www.ietf.org/rfc/rfc4718.txt

RFC4868 **Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec**
Author(s) S. Kelly, S. Frankel
Date 2007-05-01
Location http://www.ietf.org/rfc/rfc4868.txt

RFC4894 **Use of Hash Algorithms in Internet Key Exchange (IKE) and IPsec**
Author(s) P. Hoffman
Date 2007-05-01
Location http://www.ietf.org/rfc/rfc4894.txt

SP800-38A **Recommendation for Block Cipher Modes of Operation: Methods and Techniques**
Date 2001-12-01
Location https://csrc.nist.gov/publications/detail/sp/800-38a/final