Juniper Networks
Junos Space Network Management Platform, with or without Network Director and with or without Security Director in Virtual Appliance

Software: Junos Space 19.1R1_FIPS, Network-Director.3.6R3.15 and Security-Director-19.1R1.23

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Document Version: 1.0

Date: October 20, 2020

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net

Table of Contents

List of Tables

List of Figures

1 Introduction

This is a non-proprietary Cryptographic Module Security Policy for the Juniper Networks Junos Space Network Management Platform, with or without Network Director and with or without Security Director in Virtual Appliance. Junos Space Network Management Platform works with Juniper management applications to simplify and automate management of switching, routing, and security devices. As part of a complete solution, the platform provides broad fault, configuration, accounting, performance, and security management (FCAPS) capability, same day support for new devices and Junos OS releases, a task-specific user interface, and northbound APIs for integration with existing network management systems (NMS) or operations/business support systems (OSS/BSS).

Junos Space Network Director is a smart, comprehensive, and automated turnkey network management solution. Administrators can use it to visualize, analyze, and control their entire enterprise networks, all through an integrated management screen.

Junos Space Security Director provides security policy management through an intuitive, centralized interface that offers enforcement across emerging and traditional risk vectors. Using intuitive dashboards and reporting features, you gain insight into threats, compromised devices, risky applications, and more.

This FIPS 140-2 validation includes the following: the Junos Space Platform and, the Network Director (ND) and Security Director (SD) Network Management Applications. The FIPS validated version of the Junos Space software is Junos Space 19.1R1_FIPS which can be configured to operate with Junos Space Security Director and/or Junos Space Network Director i.e. the SD and/or the ND applications can be loaded onto the Junos Space Network Management Platform. The FIPS validated versions of the ND and SD are Network-Director.3.6R3.15, and Security-Director-19.1R1.23 respectively. The cryptographic implementations are in the Junos Space platform alone, the ND and SD applications do not contain any cryptographic implementations of their own.

The Junos Space software is FIPS-compliant, when configured in FIPS mode, version Junos Space 19.1R1_FIPS. The underlying operating system is CentOS 6.8 which has been hardened i.e. locked down and is thus non-modifiable. The software image is space-19.1R1.392364.ova for the Junos Space Platform, is Network-Director.3.6R3.15.img for the Network Director and Security-Director-19.1R1.23.img for the Security Director applications, respectively.

The cryptographic module is defined as a multiple-chip standalone software module. Junos Space 19.1R1_FIPS (and optionally Network-Director.3.6R3.15 and/or Security-Director-19.1R1.23) is executed on a CentOS 6.8 operating system on a VMware ESXi 6.5 Hypervisor running on a Dell PowerEdge T440 physical platform with an Intel (R) Xeon (R) Bronze 3106 CPU.

The cryptographic module was tested on the following operational environment on the hardware platform detailed in Table 1:

Table 1 – Cryptographic Module Tested Configurations

Configuration	Software Version	Operating System	Hypervisor	Processor (CPU Family)	Tested Hardware Platform
Junos Space Network Management Platform	Junos Space 19.1R1_FIPS	CentOS 6.8	VMware ESXi 6.5	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz	Dell Inc. PowerEdge T440
Junos Space Network Management Platform with Network Director	Junos Space 19.1R1_FIPS, Network-Director.3.6R3.15	CentOS 6.8	VMware ESXi 6.5	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz	Dell Inc. PowerEdge T440
Junos Space Network Management Platform with Software Director	Junos Space 19.1R1_FIPS, Security-Director-19.1R1.23	CentOS 6.8	VMware ESXi 6.5	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz	Dell Inc. PowerEdge T440
Junos Space Network Management Platform with Network Director and Software Director	Junos Space 19.1R1_FIPS, Network-Director.3.6R3.15, and Security-Director-19.1R1.23	CentOS 6.8	VMware ESXi 6.5	Intel(R) Xeon(R) Bronze 3106 CPU @ 1.70GHz	Dell Inc. PowerEdge T440

The module is designed to meet FIPS 140-2 Level 1 overall:

Table 2 – Security Level of Security Requirements

Area	Description	Level
1	Module Specification	1
2	Ports and Interfaces	1
3	Roles and Services	3
4	Finite State Model	1
5	Physical Security	N/A
6	Operational Environment	1

7	Key Management	1
8	EMI/EMC	1
9	Self-test	1
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A
	Overall	1

The module has a limited operational environment as per the FIPS 140-2 definitions. The module does not implement any mitigations of other attacks as defined by FIPS 140-2.

1.1 Cryptographic Boundary

The cryptographic boundary of the module is depicted in Figure 1 below. The physical cryptographic boundary is defined as the outer edge of the hardware server i.e. the tested platform listed in Table 1 on which the hypervisor and the module are installed. The logical boundary of the module is the space-19.1R1.392364.ova image for the Junos Space Platform (software version Junos Space 19.1R1_FIPS). The ND (Network-Director.3.6R3.15.img) and SD (Security-Director-19.1R1.23.img) applications can be optionally loaded onto the Junos Space Platform per Table 1.

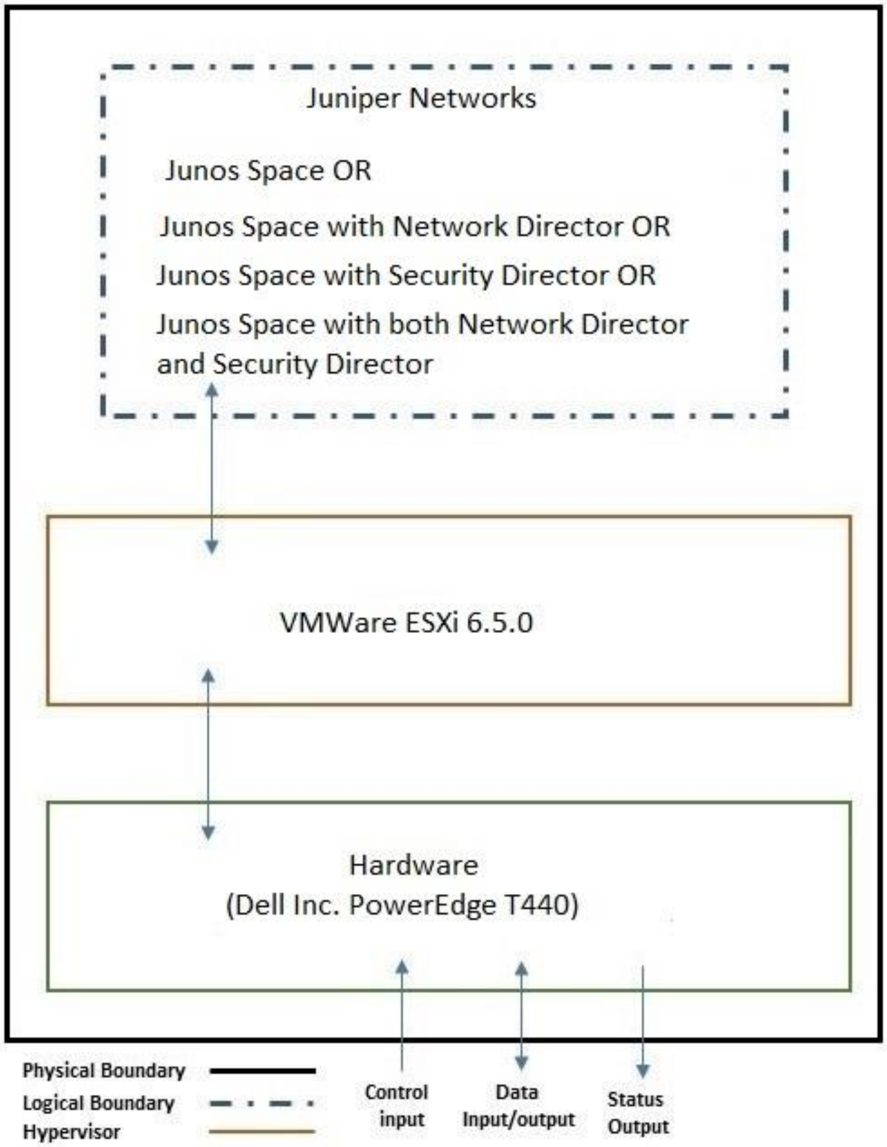

Juniper Networks
Junos Space OR
Junos Space with Network Director OR
Junos Space with Security Director OR
Junos Space with both Network Director and Security Director
VMWare ESXi 6.5.0
Hardware
(Dell Inc. PowerEdge T440)
Physical Boundary
Logical Boundary
Hypervisor
Control input
Data Input/output
Status Output

Figure 1- Module's Cryptographic Boundary

Table 3 – Ports and Interfaces

Physical Port/Interface	Logical Port/Interface	FIPS Interface
Host Platform Ethernet ports	Virtual Ethernet Ports	Data Input
Host Platform Ethernet ports	Virtual Ethernet Ports	Data Output
Host Platform Ethernet ports/ Serial port	Virtual Ethernet Ports, Virtual Serial Ports	Control Input
Host Platform Ethernet ports/ Serial port	Virtual Ethernet Ports, Virtual Serial Ports	Status Output
Power	Power	Power

1.2 Modes of Operation

The module supports one FIPS Approved mode of operation and a non-Approved mode of operation. The FIPS Approved mode of operation can only be set during the installation of the module. The module must always be zeroized when switching between the FIPS Approved mode of operation and the non-Approved mode of operation and vice versa.

1.2.1 FIPS Approved Mode

The cryptographic boundary defined in section 1, with Junos Space 19.1R1_FIPS installed, contains a FIPS-Approved mode of operation and a non-Approved mode of operation. The module is configured during initialization to operate in an approved mode or a non-approved mode.

The Crypto-Officer (CO) shall follow the instructions in Section 6.1.1 to download, install and initialize the module onto the platform identified in Table 1. Next, the module is configured in FIPS mode, by following the instructions in cryptographic officer guidance (section 6.1.2). Once the module is rebooted and the integrity and self-tests have run successfully on initial power-on in the FIPS mode, the module is operational in the FIPS-Approved mode.

1.2.2 Non-Approved Mode

The cryptographic module supports a non-Approved mode of operation. When operated in the non-Approved mode of operation, the module supports the algorithms identified in Section 2.2 as well as the algorithms supported in the Approved mode of operation.

The Crypto-Officer can place the module into a non-approved mode of operation by following the instructions in the cryptographic officer guidance (section 6.1).

1.3 Zeroization

The cryptographic module provides a non-Approved mode of operation in which non-approved cryptographic algorithms are supported. When transitioning between the non-Approved mode of operation and the Approved mode of operation, the Cryptographic Officer must zeroize all CSPs.

This is achieved by removing the Junos Space virtual machine from the datastore by following the below steps on VMWare vSphere:

1) Power off the Junos Space virtual machine
2) Ensure that another virtual machine is not sharing the disk. If two virtual machines are sharing the same disk, the disk files are not deleted
3) Right click the virtual machine and select ***All vCenter Actions > Delete from Disk***.
4) Click OK

Post zeroization, the module can be initialized by the CO in a FIPS-approved mode of operation by following the instructions in Section 6.1.2 or in a non-approved mode of operation by following the instructions in Section 6.1.3 of this document.

Note: The Cryptographic Officer must retain control of the module while zeroization is in process.

2. Cryptographic Functionality

2.1 Approved and Allowed Algorithms and Protocols

The module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in Tables 4, 5, 6, 7, 8,and 9 below. Table 10 summarizes the high-level protocol algorithm support. There are some algorithm modes that were tested but not implemented by the module. Only the algorithms, modes, and key sizes that are implemented by the module are shown in these tables.

Table 4 – OpenSSL Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1282	AES	PUB 197-38A	ECB, CBC, OFB, CFB, CTR, CCM, CMAC	Key Sizes: 128, 192, 256 bits	Encrypt, Decrypt
		SP 800-38D	GCM	Key Sizes: 128, 192, 256 bits	Encrypt, Decrypt, AEAD
C1282	SHS	PUB 180-4	SHA-1, 256, 384, 512		Message Digest Generation, KDF Primitive
			SHA-224		Message Digest Generation
C1282	DRBG	SP 800-90A	Hash, HMAC	SHA-1, 224, 256, 384, 512	Random Bit Generation
			CTR	AES-128, 192, 256	
C1282	DSA	PUB 186-4		Key sizes: 1024, 2048, 3072 bits (1024 only for SigVer)	PQG Gen, PQG Ver, Key Pair Gen, Sig Gen, Sig Ver
C1282	ECDSA	PUB 186-4		P-224,256,384,521	KeyGen, PKV
				P-224 (SHA-1[1],SHA-224,256,384,512), P-256 (SHA-1[1],224,256,384,512), P-384 (SHA-1[1],224,256,384, 512) P-521 (SHA-1[1], SHA-224, 256,384, 512)	Sig Gen, Sig Ver
N/A	KTS			AES Cert. #C1282 (modes: CBC, CTR, CFB) and HMAC Cert. #C1282	key establishment methodology provides

[1] SHA-1 is approved for SigVer alone and is not approved for SigGen.

					between 128 and 256 bits of encryption strength
				AES Cert. #C1282 (mode: AES-GCM)	key establishment methodology provides between 128 and 256 bits of encryption strength
C1282	RSA	PUB 186-4		n=2048, 3072	KeyGen
			PKCS1_V1_5, PKCSPSS, X.931	n=2048, n=3072, n=4096[2] (SHA-256, SHA-384, SHA-512)	SigGen
				n=2048, n=3072	SigVer
C1282	HMAC	PUB 198	SHA-1	Key size: 160 bits, λ = 96	Message Authentication
			SHA-224	Key size: 224 bits, λ = 224	
			SHA-256	Key size: 256 bits, λ = 128	
			SHA-384	Key size: 384 bits, λ = 384	
			SHA-512	Key size: 512 bits, λ = 512	
C1282	CVL	SP 800-135	TLS	SHA-256, 384	Key Derivation
			SNMP		
N/A[3]	KAS-SSC	SP 800-56Arev3	ECDH	P-224 (SHA 224) P-256 (SHA 256) P-384 (SHA 384) P-521 (SHA 512)	Key Agreement Scheme – Shared Secret Computation
			DH	Safe prime groups per Appendix D.	
N/A[4]	CKG	SP 800 -133rev2	Section 4		Asymmetric seed generation (for use in asymmetric key generation) using unmodified DRBG output

[2] RSA 186-4 SigGen 4096-bit modulus was not tested by the CAVP; however, it is Approved for use per CMVP guidance, because RSA 186-2 SigGen 4096-bit modulus has been tested and testing for RSA 186-4 SigGen 4096-bit modulus was not available at the time of validation.

[3] Vendor Affirmed per IG D.1rev3.

[4] Vendor Affirmed.

			Section 6.2.1	Derivation of symmetric keys

Table 5 – Bouncy Castle Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1372	AES	PUB 197-38A	ECB, CBC	Key Sizes: 128, 192, 256 bits	Encrypt, Decrypt
C1372	SHA	PUB 180-4	SHA-1, SHA-256		Message Digest Generation
C1372	DRBG	SP 800-90A	Hash	SHA-256	Random Bit Generation
C1372	DSA	PUB 186-4		Key Size: 2048	KeyPair Gen, SigGen, SigVer
C1372	ECDSA	PUB 186-4		P-256 (SHA-256)	SigGen, SigVer
C1372	RSA	PUB 186-4	PKCS1_V1_5	n=2048 (SHA 256)	SigGen, SigVer
N/A[5]	CKG	SP 800 - 133rev2	Section 4		Asymmetric seed generation (for use in asymmetric key generation) using unmodified DRBG output
			Section 6.1		Direct Generation of symmetric keys

Table 6 – OpenSSH Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1283	CVL	SP 800-135	SSH	SHA-1, SHA-256, SHA-384, SHA-512	Key Derivation

Table 7 – NSS Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1284	AES	PUB 197-38A	CBC	Key Sizes: 128 bits	Encrypt, Decrypt
C1284	SHS	PUB 180-4		SHA-256	Message Digest Generation
C1284	HMAC	PUB 198		SHA-256	Message Authentication

[5] Vendor Affirmed.

N/A	KTS			AES Cert. #C1284 (mode: CBC) and HMAC Cert. #C1284	key establishment methodology provides 128 bits of encryption strength
C1284	DRBG	SP 800-90A	Hash	SHA-256	Random Bit Generation
C1284	RSA	PUB 186-4	PKCS1_V1_5	n=2048 (SHA 256)	SigGen, SigVer
C1284	CVL	SP 800-135	TLSv1.2	SHA-256	Key Derivation

Table 8 – Linux Kernel Crypto Approved Cryptographic Functions

CAVP Cert.	Algorithm	Standard	Mode	Key Lengths, Curves, or Moduli	Functions
C1285	AES	PUB 197-38A	CBC	Key Size: 128 bits	Encrypt, Decrypt
C1285	SHS	PUB 180-4		SHA-256	Message Digest Generation
C1285	DRBG	SP 800-90A	Hash	SHA-256	Random Bit Generation

Table 9 – Allowed Cryptographic Functions

Algorithm	Caveat	Use
NDRNG [IG] 7.14 Scenario 1b	The module generates a minimum of 256 bits of entropy for key generation.	Seeding the DRBG

Table 10 – Protocols Allowed in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
SSHv2 (Server)	Diffie-Hellman (group 14 sha-1) EC Diffie-Hellman P-256, P-384, P-521	RSA 2048 ECDSA P-256, P-384, P-521	AES CBC 128/256 AES CTR 128/256	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512
HTTPS/TLS v1.2	EC Diffie-Hellman	RSA 2048	AES GCM[6] 256	AEAD (SHA-384)

[6] The AES GCM is used as part of TLS 1.2 cipher suites conformant to IG A.5, RFC 5288, and SP 800-52. The module's AES-GCM implementation conforms to IG A.5 scenario #1 following RFC 5288 for TLS. The module implements nonce management logic that ensures when the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, per RFC 5246, if the module is the party that encounters this condition it will trigger a handshake to establish a new encryption key. Per RFC 5647 the module ensures that if the invocation counter reaches its maximum value 2^64 – 1, the next

SCP (SSHv2 Client)	Diffie-Hellman (group 14, sha-1) EC Diffie-Hellman (SHA-2) P-256, P-384, P-521	RSA 2048 ECDSA P-256, P-384, P-521	AES CBC 128/256 AES CTR 128/256	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512
SNMPv3	Session Key: AES-128	HMAC-SHA-1	AES-CFB 128/192/256	

No part of these protocols, other than the KDF, have been tested by the CAVP and CMVP. The SSH algorithms allow independent selection of key exchange, authentication, cipher and integrity. In reference to the Allowed Protocols in Table 10 above: each column of options for a given protocol is independent and may be used in any viable combination. These security functions are also available in the SSH connect (non-compliant) service.

2.2 Disallowed Algorithms and Protocols

These algorithms are non-Approved algorithms that are disabled when the module is operated in an Approved mode of operation.

Algorithms

- RSA with key size less than 2048
- ECDSA with ed25519 curve
- ECDH with ed25519 curve
- ARCFOUR
- Blowfish
- CAST
- HMAC-MD5
- HMAC-RIPEMD160
- UMAC

Protocols

- Finger
- ftp
- rlogin
- telnet
- tftp
- xnm-clear-text

AES GCM encryption is performed with the invocation counter set to either 0 or 1, with a maximum of 2^64 – 1 encryptions per session.

2.3 Critical Security Parameters

All CSPs and public keys used by the module are described in this section.

Table 11 – Critical Security Parameters (CSPs)

Name	Description and usage
DRBG_Seed	Seed material used to seed or reseed the DRBG
DRBG_State	V and Key values for the HMAC_DRBG
Entropy Input String	256 bits entropy (min) input used to instantiate the DRBG
SSH PHK	SSH Private host key. 1st time SSH is configured, the keys are generated. RSA 2048, ECDSA P-256, P-384, P-512. Used to identify the host.
SSH DH	SSH Diffie-Hellman private component. Diffie-Hellman private key used in SSH. DH (group 14, sha-1).
SSH ECDH	SSH Elliptic Curve Diffie-Hellman private component. Ephemeral Diffie-Hellman private key used in SSH. ECDH P-256, or ECDH P-384 or ECDH P-521
ECDH Shared Secret	The Diffie-Hellman shared secret used in EC Diffie-Hellman (ECDH) exchange. Created per the EC Diffie-Hellman protocol. Provides between 128-256 bits of security.
DH Shared Secret	The Diffie-Hellman shared secret used in EC Diffie-Hellman (ECDH) exchange. Created per the EC Diffie-Hellman protocol. Provides between 128-256 bits of security.
SSH-SEKs	SSH Session Keys: SSH Session Encryption Key: AES; SSH Session Integrity Key: HMAC
SNMPv3 Password	Shared secret used to derive HMAC-SHA1 key for SNMPv3 Authentication
SnmpEngineID	Unique string to identify the SNMP engine.
SNMPv3 session key	SNMPv3 Session Key: AES-128. Used to encrypt the SNMPv3 traffic.
HTTPS Pre-Master secret	Shared Secret used to to derive the master secret (create HTTPS session keys).
HTTPS Master secret	Shared Secret used to create HTTPS session keys.
HTTPS SEKs	HTTPS Session Keys: HTTPS Encryption Key: AES-GCM-256; HTTPS Integrity Key: AEAD (SHA-384).
TLS Pre-Master secret	Shared Secret used to derive the master secret (create TLS session keys).
TLS Master secret	Shared Secret used to create TLS session keys.
TLS-SEKs	TLS Session Keys: TLS Encryption Key: AES-GCM-256; TLS Integrity Key: AEAD (SHA-384).
TLS RSA private key	RSA 2048
CO-PW	ASCII Text used to authenticate the CO.
User-PW	ASCII Text used to authenticate the User.

Table 12– Public Keys

Name	Description and usage
SSH-PUB	SSH Public Host Key. RSA 2048, ECDSA P-256, P-384, P-521. Used to identify the host.
SSH-DH-PUB	Diffie-Hellman public component. Diffie-Hellman public key used in SSH key establishment. DH (group 14, SHA-1)
SSH-ECDH-PUB	Elliptic Curve Diffie-Hellman public component. Ephemeral EC Diffie-Hellman public key used in SSH key establishment. ECDH P-256, ECDH P-384 or ECDH P-521
TLS RSA public key	RSA 2048

3. Roles, Authentication and Services

3.1 Roles and Authentication of Operators to Roles

The module supports two roles: Cryptographic Officer (CO) and User. The module supports concurrent operators via the GUI but does not support a maintenance role or any bypass capability. The module enforces the separation of roles using the identity-based operator authentication method as described in section 3.2.

The Cryptographic Officer role configures and monitors the module via the GUI, a console or SSH connection.

The User role monitors the module via the GUI alone. The user role may not initialize the module.

3.2 Authentication Methods

The module implements two forms of Identity-Based authentication, Username and password over the CLI (Console and SSH) for the CO role and Username and password over the GUI for both the CO and user roles.

Password authentication (GUI): The module enforces 6-character passwords (at minimum) chosen from the 96 human readable ASCII characters. Thus, the probability of a successful random attempt is 1/(96^6), which is less than 1/1 million.

The passwords must contain at least one lowercase character and one number. The passwords must not repeat or reverse the Login ID, contain more than three repetitive characters or end in a number.

Password authentication (Console/SSH i.e. CLI): A password or passphrase can be set for the CO role over the CLI. A valid password should be a mix of upper and lower case letters, digits, and other characters. An 8 character-long password with characters from at least 3 of these 4 classes can be used chosen from the 96 human readable ASCII characters. Thus, the probability of a successful random attempt is 1/(96^8), which is less than 1/1 million. An uppercase letter that begins the password and a digit that ends it do not count towards the number of character classes used, unless the "disable_firstupper_lastdigit_check" option is enabled.

A passphrase should be of at least 3 words, 16 to 40 characters long, and contain enough different characters, thus enforcing a 48 character-long password at minimum. Thus, the probability of a successful random attempt is 1/(96^48), which is less than 1/1 million.

The module enforces a timed access mechanism as follows: For the first two failed attempts (assuming 0 time to process), no timed access is enforced. Upon the third attempt, the module enforces a 5-second delay. Each failed attempt thereafter results in an additional 5-second delay above the previous (e.g. 4 th failed attempt = 10-second delay, 5 th failed attempt = 15-second delay, 6 th failed attempt = 20-second delay, 7 th failed attempt = 25-second delay). This leads to a maximum of 7 possible attempts in a one-minute period for each getty. The best approach for the attacker would be to disconnect after 4 failed attempts and wait for a new getty to be spawned. This would allow the attacker to perform roughly 9.6 attempts per minute (576 attempts per hour/60 mins); this would be rounded down to 9 per minute, because there is no such thing as 0.6 attempts. The probability of a success with multiple consecutive attempts in a one-minute period is 9/(96^6), which is less than 1/100,000.

3.3 Approved and Allowed Services

All services implemented by the module are listed in the tables below.

Table 15 lists the access to CSPs by each service.

Table 13 – Authenticated Services

Service	Description	CO	User
Configure security	Security relevant configuration	X	
Configure	Non-security relevant configuration	X	X
Status	Show status	X	X
Zeroize	Destroy all CSPs	X	
SSH connect (inbound)	Initiate SSH connection for SSH monitoring and control (CLI) of the module	X	
SSH connect (outbound)	Initiate SSH connection for SSH monitoring and control of external network devices (CLI)	X	X
Console access	Console monitoring and control (CLI)	X	
HTTPS	Initiate an HTTPS connection for monitoring and control (GUI)	X	X
SCP	Secure copy for backups and recovery	X	X
SNMPv3	Remote monitoring of external network devices	X	X
TLS (Syslog)	Used to encrypt syslog messages	X	X
TLS (MySQL, Postgres)	Used to encrypt connections/access to the databases	X	X
Remote reset Load Image	Software initiated reset. Used to perform self-tests on demand Verification and loading of a validated firmware image.	X X	

Table 14 – Unauthenticated service

Service	Description
Local reset	Hardware reset or power cycle

Table 15 – CSP Access Rights within Services

Service	CSPs																				
	DRBG_Seed	DRBG_State	Entropy Input	ECDH Shared	DH Shared	SSH PHK	SSH ECDH	SSH DH	SSH-SEK	snmpEngineID	SNMPv3	SNMPv3	HTTPS/TLS Pre-	HTTPS/TLS	HTTPS TLS-SEKs	TLS Pre-Master	TLS Master	TLS-SEKs	TLS RSA private	CO-PW	User-PW

Configure security	--	E	--	G W R	G W R	G W R	--	--	--	W R	W R	--	W	W	--	W	W	--	G W R	W	W
Configure	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Status	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
SSH connect (inbound)	--	E	--	E	E	E	G E	G E	G E	--	--	--	--	--	--	--	--	--	--	E	--
SSH connect (outbound)	--	E	--	E	E	E	G E	G E	G E	--	--	--	--	--	--	--	--	--	--	E	E
Console access	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--
HTTPS	--	E	--	E	--	--	--	--	--	--	--	--	E	E	G E	E	E	G E	E	E	E
SCP	--	E	--	E	E	E	G E	G E	G E	--	--	--	--	--	--	--	--	--	--	E	E
SNMP v3	--	--	--	--	--	--	--	--	--	E	E	G E	--	--	--	--	--	--	--	E	E
TLS v1.2	--	E	--	E	E	--	--	--	--	--	--	--	--	--	--	E	E	G E	E	E	E
Remote reset	G E Z	G Z	G Z	Z	Z	--	Z	Z	Z	--	--	Z	Z	Z	Z	Z	Z	Z	--	--	--
Local reset	G E Z	G Z	G Z	Z	Z	--	Z	Z	Z	--	--	Z	Z	Z	Z	Z	Z	Z	--	--	--
Load Image	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

G = Generate: The module generates the CSP
R = Read: The CSP is read from the module (e.g. the CSP is output)
E = Execute: The module executes using the CSP
W = Write: The CSP is updated or written to the module
Z = Zeroize: The module zeroizes the CSP.

3.4 Non-Approved Services

The following services are available in the non-Approved mode of operation. The security functions provided by the non-Approved services are identical to the Approved counterparts with the exception of SSH Connect (non-compliant). SSH Connect (non-compliant) supports the security functions identified in Section 2.2and the SSHv2 row of Table 10.

Table 16 – Authenticated Services

Service	Description	CO	User
Configure security (non-compliant)	Security relevant configuration	X	
Configure (non-compliant)	Non-security relevant configuration	X	X
Status (non-compliant)	Show status	X	X
Zeroize (non-compliant)	Destroy all CSPs	X	
SSH connect (inbound) (non-compliant)	Initiate SSH connection for SSH monitoring and control (CLI) of the module	X	
SSH connect (outbound) (non-compliant)	Initiate SSH connection for SSH monitoring and control of external network devices (CLI)	X	X
Console access (non-compliant)	Console monitoring and control (CLI)	X	
HTTPS (non-compliant)	Initiate an HTTPS connection for monitoring and control (GUI)	X	X
SCP (non-compliant)	Secure copy for backups and recovery	X	X
SNMPv3 (non-compliant)	Remote monitoring of external network devices	X	X
TLS (Syslog) (non-compliant)	Used to encrypt syslog messages	X	X
TLS (MySQL, Postgres) (non-compliant)	Used to encrypt connections/access to the databases	X	X
Remote reset (non-compliant) Load Image (non-compliant)	Software initiated reset. Used to perform self-tests on demand. Verification and loading of a validated firmware image.	X X	

Table 17– Unauthenticated service

Service	Description
Local reset (non-compliant)	Hardware reset or power cycle

4. Self-tests

Each time the module is powered up, it tests that the cryptographic algorithms still operate correctly, and that sensitive data have not been damaged. Power-up self–tests are available on demand by power cycling the module.

On power-up or reset, the module performs the self-tests described below. All KATs must be completed successfully prior to any other use of cryptography by the module. If one of the KATs fails, the module enters the Critical Failure error state.

The module performs the following power-up self-tests:

- Software Integrity check using HMAC-SHA256

- OpenSSL KATs
  - SP 800-90A HMAC DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - SP 800-90A Hash DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - SP 800-90A CTR DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - ECDSA Sign/Verify PCT
  - RSA Sign/Verify KAT
  - HMAC-SHA-1 KAT
  - HMAC-SHA-224 KAT
  - HMAC-SHA-256 KAT
  - HMAC-SHA-384 KAT
  - HMAC-SHA-512 KAT
  - AES-CBC (128/192/256) Encrypt KAT
  - AES-CBC (128/192/256) Decrypt KAT
  - AES-CMAC (128/192/256) KAT
  - AES-GCM (128) KAT
  - DSA Sign/Verify KAT

- Bouncy Castle KATs
  - AES-ECB (128) Encrypt/Decrypt KAT
  - SHA-1 KAT
  - SHA-256 KAT
  - SP 800-90A Hash DRBG KAT
    - Health-tests initialize, re-seed, and generate
  - DSA 2048 Sign/Verify KAT
  - ECDSA P-256 Sign/Verify KAT
  - RSA 2048 Sign/Verify KAT

- NSS
  - AES-CBC (128) Encrypt KAT
  - AES-CBC (128) Decrypt KAT
  - HMAC-SHA-256 KAT

- SP 800-90A Hash DRBG KAT
    - Health-tests initialize, re-seed, and generate
- RSA w/ SHA-256 Sign/Verify KAT

- Linux Kernel Crypto
    - AES-CBC (128) Encrypt KAT
    - AES-CBC (128) Decrypt KAT
    - SHA-256 KAT
    - SP 800-90A Hash DRBG KAT

Health-tests initialize, re-seed, and generate

The module also performs the following conditional self-tests:

- Continuous RNG Test on the SP 800-90A HMAC-DRBG, Hash-DRBG and CTR DRBG for the OpenSSL library and Hash-DRBG for the Bouncy Castle, NSS and Linux Kernel Crypto libraries.
- Continuous RNG test on the NDRNG.
- Pairwise consistency test when generating DSA, ECDSA, and RSA key pairs.
- Software Load Test (HMAC-SHA256 signature verification) on the Junos Space platform, as well as a Software load test (RSA2 SHA-256 signature verification) on the ND and SD applications.

5. Physical Security Policy

The module’s physical security requirements do not apply s because the module is a FIPS 140-2 Level 1 software module and the physical security is provided by the tested host platform.

6. Security Rules and Guidance

The module design corresponds to the security rules below. The term *must* in this context specifically refers to a requirement for correct usage of the module in the Approved mode; all other statements indicate a security rule implemented by the module.

1. The module clears previous authentications on power cycle.
2. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
3. Power up self-tests do not require any operator action.
4. Data output is inhibited during key generation, self-tests, zeroization, and error states.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module does not support a maintenance interface or role.
8. The module does not support manual key entry.
9. The module does not output intermediate key values.
10. The module does not support output of plaintext CSPs.
11. The cryptographic officer must retain control of the module while zeroization is in process.

    12. If the module loses power and then it is restored, then a new key shall be established for use with the AES GCM encryption/decryption processes.13. The cryptographic officer shall verify that the Junos Space software image as well as the ND and SD applications which can be loaded on the module are the FIPS validated images. If any non-validated software image or application is loaded the module will no longer be a FIPS validated module.

14.. The cryptographic officer shall verify that the Junos Space Platform is configured as a single Space node i.e. the Junos Space Platform comprising of the full functionality. If any other type of node or multiple nodes in a cluster are configured, the module will no longer be a FIPS validated module.

6.1 Crypto-Officer Guidance

The crypto-officer is responsible for installing the module on the hardware platform on which the module was tested and validated, configuring the module in FIPS mode and configuring the operator's usernames and passwords.

The crypto-officer shall follow the instructions for uploading/ installing Junos Space, the ND and the SD images provided in the *Juniper Networks Junos Space Network Management Platform FIPS Evaluated Configuration Guide for Junos Space*, *Release 19.1R1* and the *Juniper Networks Junos Space Network Management Platform Complete Software Guide, Release 19.1R1* documentation. The steps mentioned therein have been listed as follows:

6.1.1 Installing the FIPS-Approved software image

Guide to Download Software Packages for Junos Space & the ND/SD Applications from Juniper Networks:

1. Using a Web browser, follow the link to the download URL on the Juniper Networks webpage at https://www.juniper.net/support/products/space/#sw
2. Log in to the Juniper Networks website using the username (generally your e-mail address) and password supplied by your Juniper Networks representatives.
3. Under "Version" dropped down list, select the appropriate certified Release (Example: 19.1R1).
4. Under "Application Media" section, select the appropriate software package for the target release version and hypervisor.
5. Download the Junos Space, ND and SD images to a local host or to an internal software distribution site.
6. SHA256 checksum can be found under "Checksum"
    - Verify the checksum of the download with the provided checksum

Installing the Junos Space Platform:

The deployment of a Junos Space Virtual Appliance i.e. the Junos Space Platform on a VMware ESXi server includes the following tasks:

1. Install the VMware ESXi Server.

2. Install the Junos Space Virtual Appliance on the VMware ESXi Server:

You can use vSphere Client 6.5 or later or OVF Tool 2.01 or later to deploy the Junos Space Virtual Appliance image on a VMWare ESXi server.

To create a Junos Space Virtual Appliance by using vSphere Client 6.5:

1. Download the Junos Space Virtual Appliance image from https://www.juniper.net/support/downloads/?p=space#sw to your local system.

Launch the vSphere Client that is connected to the ESXi server where the Junos Space Virtual Appliance is to be deployed.

3. Select File > Deploy OVF Template from the menu bar.

The Deploy OVF Template page appears.

4. Click the Deploy from file option and click Browse, and then upload the OVA file from your ` storage location

5. Click Next.

6. Verify the OVF Template details and then click Next.

7. Specify a name and location for the deployed template and then click Next.

A template name can contain a maximum of 80 characters. Template names are not case-sensitive.

8. Verify your settings and then click Finish to create the Junos Space Virtual Appliance.

To create a Junos Space Virtual Appliance by using the OVF Tool:

1. Download the Junos Space Virtual Appliance image from https://www.juniper.net/support/downloads/?p=space#sw to your local system.

2. Login to the local system and navigate to the location where the Junos Space Virtual Appliance image file is saved.

3. Run the following command:

```
/usr/bin/ovftool/ovftool --name=virtual-appliance image-file vi://username:password@host-id
```

where:

• virtual appliance is the name you assign to the Junos Space Virtual Appliance.

• image-file is the name of the Junos Space Virtual Appliance image file.

• username is the username of the host machine where you deploy the Junos Space Virtual Appliance.

• password is the password of the host machine where you deploy the Junos Space Virtual Appliance.

• host-id is the IP address of the host machine where you deploy the Junos Space Virtual Appliance.

Example:

```
/usr/bin/ovftool/ovftool-name=space1vmspace-19.1R1.ova
vi://username:password@10.157.10.1
```

The Junos Space Virtual Appliance is deployed on the host machine.

4. Log in to the host machine and edit the settings (number of processors, memory) of the Junos Space Virtual Appliance. For information about editing the settings of a Junos Space Virtual Appliance by using the OVF Tool, see the OVF Tool documentation at https://www.vmware.com/support/developer/ovf/.

3. Modifying RAM Settings for a Junos Space Virtual Appliance:

To add RAM for a Junos Space Virtual Appliance:

1. Launch the VMware vSphere Client and log in to the ESXi server where the Junos Space Virtual Appliance is deployed.

2. Select the Junos Space Virtual Appliance from the inventory view.

3. IftheJunosSpaceVirtualApplianceispoweredon,youmustpowerofftheappliance to configure RAM.

To power off the Junos Space Virtual Appliance, right-click the Junos Space Virtual Appliance icon and select Power > Power Off.

4. Select the Summary tab to view the Junos Space virtual machine settings.

5. Select EditSettings to view and edit the virtual memory settings.

6. Select Memory.

7. Update the RAM to 32 GB to operate the Junos Space Virtual Appliance as a Junos Space node.

8. Click OK.

RAM is added to the Junos Space Virtual Appliance.

4. Adding Disk Resources for a Junos Space Virtual Appliance:

The Junos Space Virtual Appliance files are distributed with 250-GB of disk space.

To allocate additional disk space for partitions, add a disk resource and expand a partition one at a time. The free space available on the disk resource can be shared among the different partitions. For example, to expand the /var and /var/log partitions by 20 GB each, add a disk resource of minimum 40 GB. Expand the drive size of the /var partition by 20 GB and then expand the /var/log partition by 20 GB.

The Junos Space Virtual Appliance file is distributed with 250 GB of disk space. You can increase the hard disk size based on the requirement for the specific Junos Space deployment. The following procedure describes how you can add disk resources for a Junos Space Virtual Appliance deployed on a VMware ESX or VMware ESXi Server.

To add disk resources for the Junos Space Virtual Appliance:

1. IntheVMwarevSphereClient,right-clicktheJunosSpaceVirtualApplianceiconand select Power > Power On. The Junos Space Virtual Appliance must be powered on to add disk resources.

2. Right-click the Junos Space Virtual Appliance icon and select Edit Settings.

The Virtual Machine Properties page is displayed.

3. Select the Hardware tab and click Add.

The Device Type page is displayed.

4. Under Choose the type of disk you wish to add, select Hard Disk.

5. Click Next.

The Select a Disk page appears.

6. Under Disk, select Create a new Virtual disk.

7. Click Next.

The Create a Disk page appears.

8. Under Capacity, set the Disk Size field to the recommended size for the partition that you want to expand.

Under Location, retain the default setting—that is, leave the Store with the virtual machine selected.

9. Click Next.

The Advanced Options page is displayed.

10. Leave the default settings unchanged and click Next.

The Ready to Complete page is displayed.

11. Review your selected options and click Finish.

The Virtual Machine Properties page displays the new virtual disk on the Hardware list.

12. Click OK to create the new virtual disk.

A status bar shows the progress at the bottom of the page.

Once this has completed, the CO can then initialize the module in a FIPS approved mode of operation by following steps in Section 6.1.2 or a non-approved mode of operation following the steps in Section 6.1.3 of this document respectively.

Adding a Junos Space Application:

The administrator can add a new Junos Space application (Network Director or Security Director) while Junos Space Network Management Platform is still running. This can be done either in the FIPS mode of operation or in the non-FIPS mode of operation. The procedure in either case is as follows:

Adding an application to the Junos Space Platform server is a two-step process:
1. Upload the application to the Junos Space Platform server.
2. Install the uploaded application.

Uploading the Junos Space Application

To upload a Junos Space application:
1. Ensure that the Junos Space application you want to add is downloaded from the Juniper Networks software download site to the local client file system: https://www.juniper.net/support/products/space/#sw

2. Select Administration > Applications and click the Add Application icon. The Add Application page appears. If you have not uploaded any applications, the page is blank.

3. Upload the new application by performing one of the following steps:
a. Click Upload via HTTP.
The Software File dialog box appears.
i. Type the name of the application file or click Browse to navigate to where the new Junos Space application file is located on the local file system.
ii. Click Upload. This action might take a while. Wait until the application is uploaded.

b. Click Upload via SCP.
The Upload Software via SCP dialog box appears. Add the Secure Copy credentials to upload the Junos Space Platform application image from a remote server to Junos Space.
i. In the Username field, enter your username.
ii. In the Password field, enter your password.
iii. In the Confirm password field, enter your password again to confirm the password.
iv. In the Machine IP field, enter the host IP address.
v. In the Software File Path field, enter the path name of the Junos Space

application file.
For example, /root/<*image-name*>.img.
vi. Click Upload. This action might take a while. Wait until the application is uploaded.

4. In the Application Management Job Information dialog box, if you click the Job ID link, you see the Add Application job on the Jobs > Job Management inventory page. Wait until the job is completed and ensure that the job is successful.
If the upload is successful, then the new application is displayed by application name, filename, version, release level, and the required Junos Space Platform version on the Add Application page.

Installing the Uploaded Junos Space Application

To install the uploaded application:
1. Select Administration > Applications and click the Add Application icon.
The Add Application page appears.

2. Select the uploaded application.

3. Click Install to install the application or click Cancel to exit the Add Application page.
The Application configuration page appears, displaying a list of server groups to which you can deploy the application.

4. Select a server group to which you want to deploy the application. The default server group is platform to which Junos Space Platform is deployed. If you do not select any server group, the selected application is automatically deployed to the default platform server group.

5. Click OK to proceed.
The Application Management Job Information dialog box appears.

6. In the Application Management Job Information dialog box, if you click the Job ID link, you see the Add Application job on the Job Management page. Wait until the application is fully deployed and ensure that the job is successful.
If the installation of the application is a failure, then the Summary column for the installation job displays the reason for failure. However, the display of messages depends also on the type and version of the application being installed.

7. If the installation is successful, without logging out of Junos Space Platform, select the application from the Application Chooser list (located at the top-left) to view and begin using its workspaces and tasks.

6.1.2 Enabling FIPS-Approved Mode of Operation

The cryptographic officer is responsible for initializing the module in a FIPS-Approved mode of operation. The FIPS-Approved mode of operation is not automatically enabled and can only be enabled during the installation process of Junos Space The cryptographic officer shall follow the steps found in the *Juniper Networks Junos Space Network Management Platform FIPS Evaluated Configuration Guide for Junos Space, Release 19.1R1* document to place the module into a FIPS-Approved mode of operation.

The steps from the aforementioned document are repeated below:

To enable FIPS mode in Junos OS on the module:

During the Junos Space installation, the user will be promoted whether to install the node in FIPS mode or not. If the user chooses FIPS mode, then appropriate configuration changes will be done, Junos Space files would be indexed for Post Integrity Tests and the Space server will be rebooted to make the changes reflect.

There are two types of nodes for Junos Space, namely the Space and FMPM nodes. The Space node is the Junos Space Platform comprising of the full functionality. Every Junos Space Installation requires at least one Space node. The FMPM node is catered to fault and performance monitoring only. For this validation the Space node i.e. the Junos Space Platform has been tested. The “Do you want to enable FIPS mode” question will be prompted for all types of Space nodes (Space/DB/FMPM) installation. Only a FIPS enabled node can be added in a FIPS enabled setup and only a FIPS disabled node can be added in a FIPS disabled setup.

The steps for initializing the module are as follows:

1. Access the console on the virtual machine client to view the Junos Space login prompt.

2. At the Junos Space login prompt, type admin as your default login name and press Enter.

```
space-node login:admin
Password:
```

3. You are prompted to enter the administrator password. Type abc123 as the default administrator password and press Enter. Junos Space prompts you to change your default password.

4. To change the default password, do the following:

- Type the default password and press Enter.
- Type your new password and press Enter.
- Retype your new password and press Enter.

If the password is changed successfully, the following message is displayed.

```
passwd: all authentication tokens updated successfully
```

Enter the new password to log in to Junos Space.

5. Type S to install the virtual appliance as a Junos Space node.

```
This Junos Space node can be installed as one of the following:
(S)pace Platform

Full functionality. Every Junos Space Installation requires at least one Space
 node.
```

```
(F)MPM

Specialized to fault and performance monitoring only. This requires at least
one Space node.
```

```
Choose the type of node to be installed [S/F] S
```

6. After setting the general network settings, the module provides the option to enable the FIPS mode of operation:

Note: Enabling FIPS mode is a one-time activity and it can be done only at the installation.

Do you want to enable FIPS mode of Space installation? [y/N] y . . .

Entering “y” above will enable the FIPS mode of operation on the module.

7. Once all the required settings have been selected, a summary of the same is printed by the module on the CLI which indicates the following:

> FIPS mode is enabled

A> Apply settings
C> Change settings
Q> Quit and set up later
R> Redraw Menu
. . . FIPS mode enabled successfully.
Node will be rebooted in 2 minutes

8. The CO can verify that the FIPS mode has been enabled as follows:

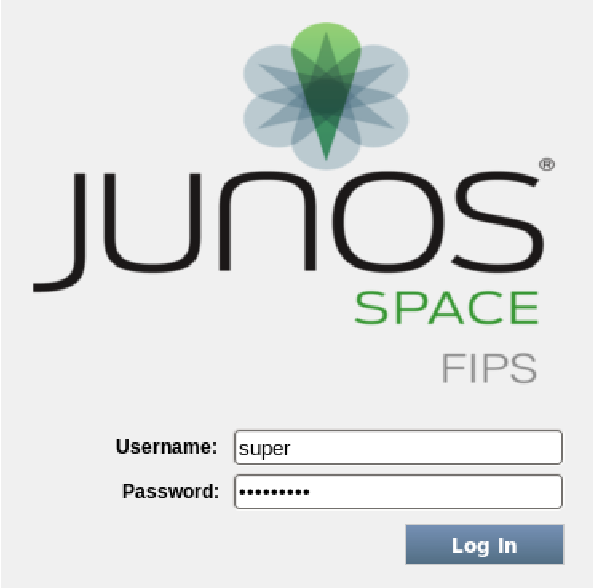
- **CLI:**

  FIPS mode status is stored in the file - /etc/sysconfig/JunosSpace/jmp-fips, if it contains zero value/empty then the node is running in Non-FIPS mode. A value of one (1) is indicative of the FIPS Approved mode of operation.

  Junos Space FIPS mode will be shown in SSH Banner message as below
  [vignesh@vignesh Desktop]$ ssh admin@10.1.2.198
  Space release 19.1R1.391908 (391908)

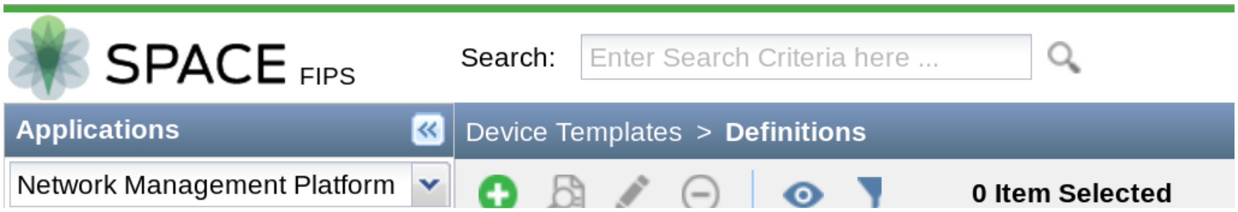
admin@10.1.2.198 's password:

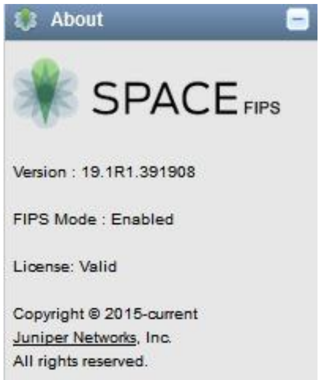
- **GUI:**
  Junos Space FIPS mode will be shown on the GUI in the following places.
  1. Junos Space Logo in Login/Logout screens
  2. Junos Space Icon in top left corner of GUI
  3. Help -> About page.



Username: super

Password: •••••••••


SPACE FIPS
Search:
Enter Search Criteria here ...
Applications
Network Management Platform
Device Templates > Definitions
0 Item Selected



Version : 19.1R1.391908

FIPS Mode : Enabled

License: Valid

Copyright © 2015-current
Juniper Networks, Inc.
All rights reserved.

- **JVM(Jboss):** FIPS mode can be verified by the CO role from the java system property 'FIPSMode' via the CLI. The value would be true when Junos Space is installed in FIPS mode.

Adding ND/SD Applications to Junos Space in the FIPS mode:

Enabling FIPS mode of operation on the Junos Space platform, automatically enables FIPS mode on the ND and SD applications when they are installed on the Junos Space platform.

The steps for adding the ND and/or SD applications to the Junos Space platform are as outlined in section 6.1.1 (Adding a Junos Space Application) above.

6.1.3 Placing the Module in a Non-Approved Mode of Operation

As cryptographic officer, the operator may need to place the module from the FIPS-Approved mode of operation to a non-Approved mode of operation by zeroizing the module. Follow the steps found in section 1.3 to zeroize the module.

Once the zeroization process has been completed, the operator as the CO can then do the following so as to initialize the module in a non-Approved mode of operation:

During the Junos Space initialization, user will be prompted whether to install the node in FIPS mode or not. If the user does not choose the FIPS mode, then the non-approved mode of operation will be enabled.

There are two types of nodes for Junos Space, namely the Space and FMPM nodes. The Space node is the Junos Space Platform comprising of the full functionality. Every Junos Space Installation requires at least one Space node. The FMPM node is catered to fault and performance monitoring only. For this validation the Space node i.e. the Junos Space Platform has been tested. The “Do you want to enable FIPS mode” question will be prompted for all types of Space nodes installation.

To enable the non-approved mode of operation:

1. Follow Steps 1 through 5 outlined in Section 6.1.2 of this document.

2. Select the “N” option as below:

Do you want to enable FIPS mode of Space installation? [y/N]: N

You have chosen for fresh installation, FIPS mode will not be enabled. Do you want to still proceed with Space normal mode installation? [y/N]: N

Normal mode Installation Continued...!

3. Once all the required settings have been selected, a summary of the same is printed by the module on the CLI which indicates does not have the “FIPS mode is enabled” entry thus indicating that the non-approved mode of operation has been enabled.

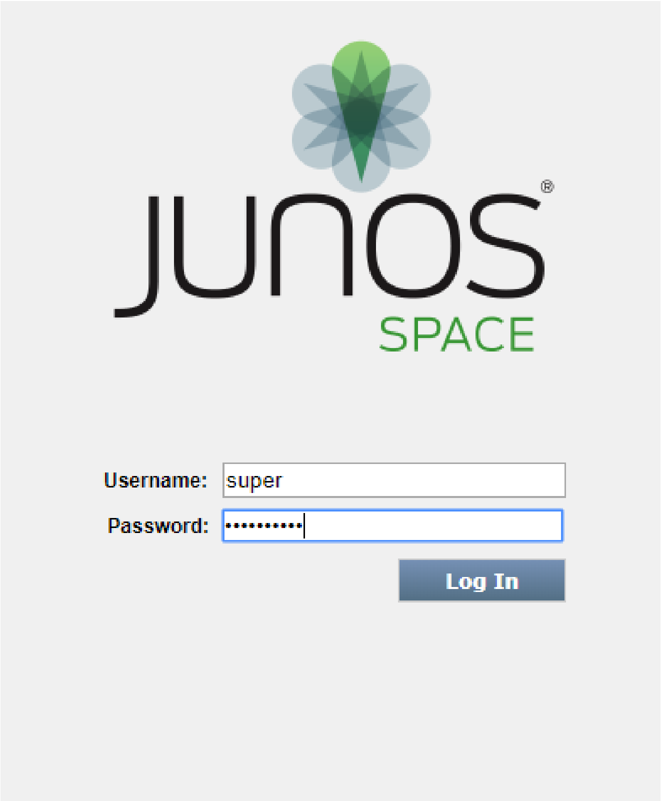
4. The CO can verify that the non-FIPS mode has been enabled as follows:

- **CLI:**
  FIPS mode status is stored in the file - /etc/sysconfig/JunosSpace/jmp-fips, if it contains zero value/empty then the node is running in Non-FIPS mode.

- **SSH:**
  Junos Space non-FIPS mode can be verified from the SSH Banner message as below, the lack of the "(FIPS)" identifier indicates that it is in a non-FIPS mode of operation:

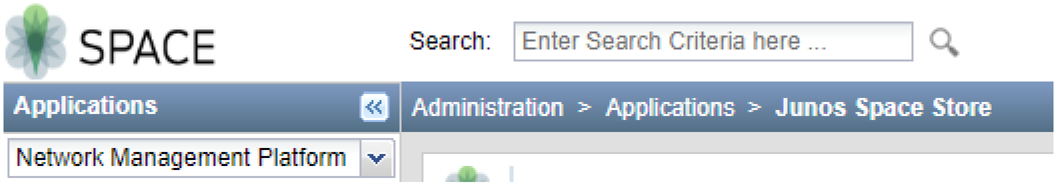
  ```
  [vignesh@vignesh Desktop]$ ssh admin@10.1.2.198
  Space release 19.1R1.391908 (391908)
  admin@10.1.2.198 's password:
  ```

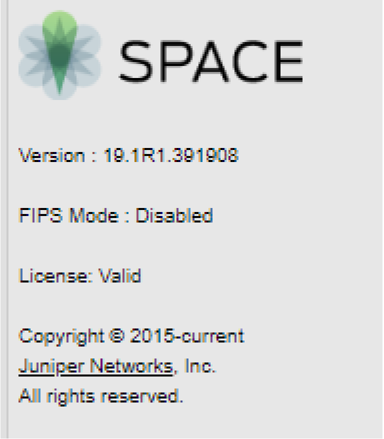
- **GUI:**
  Junos Space non-FIPS mode will be indicated in the GUI in the following places, the lack of the "(FIPS)" identifier indicates that it is in a non-FIPS mode of operation:
  - Junos Space Logo in Login/Logout screens
  - Junos Space Icon in top left corner of GUI
  - Help -> About page.



Username: super

Password: ••••••••••


SPACE
Search: Enter Search Criteria here ...
Applications
Network Management Platform
Administration > Applications > Junos Space Store



Version : 19.1R1.391908

FIPS Mode : Disabled

License: Valid

Copyright © 2015-current
Juniper Networks, Inc.
All rights reserved.

- **JVM(Jboss):** FIPS mode can be verified by the CO from the java system property 'FIPSMode' via the CLI. The value would be false when Junos Space is installed in the non-FIPS mode.

Adding ND/SD Applications to Junos Space in the non-FIPS mode:

Not enabling the FIPS mode of operation on the Junos Space platform, automatically initializes the ND and SD applications in the non-FIPS mode when they are installed on the Junos Space platform.

The steps for adding the ND and/or SD applications to the Junos Space platform are as outlined in section 6.1.1 (Adding a Junos Space Application) above.

7. References and Definitions

The following standards are referred to in this Security Policy.

Table 18 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Module*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.

Table 19 – Acronyms and Definitions

Acronym	Definition
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic Compatibility
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
IKE	Internet Key Exchange Protocol
IPsec	Internet Protocol Security
MD5	Message Digest 5
RSA	Public-key encryption technology developed by RSA Data Security, Inc.
SHA	Secure Hash Algorithms
SSH	Secure Shell

Table 20 – Datasheets

Model	Title	URL
Junos Space	Junos Space	https://www.juniper.net/us/en/local/pdf/datasheets/1000297-en.pdf
Network Director	Junos Space Network Director	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000428-en.pdf
Security Director	Junos Space Security Director	https://www.juniper.net/assets/us/en/local/pdf/datasheets/1000332-en.pdf