BIG-IP® Common Criteria Evaluation Configuration Guide

BIG-IP® Release 16.1.3.1
Including SSLO

Document Number: CC2021-AGD-002
Document Version: 6.17
Date: 12/5/2023

Table of Contents

Table of Tables

1 Introduction

This document is the customer guidance supplement for configuration and use of the NDcPP+STIP PPM (Network Device collaborative Protection Profile + SSL/TLS Inspection Proxy Protection Profile Module) evaluated configurations for BIG-IP Release 16.1.3.1 including SSLO (Secure Socket Layer Orchestrator).

This document includes a description of the evaluated configuration.

NOTE: This document, along with *K76615426 Common Criteria Certification for BIG-IP 16.1.3.1*, provides guidance on the secure installation and secure use of the TOE (Target of Evaluation) for the evaluated configuration. This document provides clarifications and changes to the standard documentation and should be used as the guiding document for the configuration and administration of the TOE in the Common Criteria evaluated configuration. Official product documentation should be referred to and followed only as directed within this guiding document.

1.1 References

All of the documents in the table below are applicable to the current TOE release as described in this document. However, some documents have not been updated for the current release and still reflect prior releases in their names.

Certification-specific References
K76615426: Common Criteria Certification for BIG-IP 16.1.3.1
BIG-IP including SSLO: ***F5 BIG-IP 16.1.3.1 including SSLO Security Target***
General BIG-IP References
BIG-IP Device Service Clustering: Administration
BIG-IP Digital Certificates: Administration
BIG-IP Local Traffic Manager: Implementations
BIG-IP Local Traffic Manager: Monitors Reference
BIG-IP Local Traffic Manager: Profiles Reference
BIG-IP Local Traffic Manager: Configuring a Custom Cipher String for SSL Negotiation
BIG-IP Release Note
BIG-IP System: Essentials
BIG-IP System: SSL Administration
BIG-IP System: User Account Administration
BIG-IP Systems: Getting Started Guide
BIG-IP TMOS: Implementations
BIG-IP TMOS: Routing Administration
External Monitoring of BIG-IP Systems: Implementations
GUI Help Files
iControl API Reference
iControl REST API User Guide
K08859735: Overview of the FTP profile (14.x – 16.x)

K12042624: Restricting access to the Configuration utility using client certificates (13.x – 16.x)
K13092: Overview of securing access to the BIG-IP system
K13123: Managing BIG-IP product hotfixes (11.x – 17.x)
K13302: Configuring the BIG-IP system to use an SSL chain certificate (11.x – 16.x)
K13454: Configuring SSH public key authentication on BIP-IP systems (11.x – 16.x)
K14620: Managing SSL Certificates for BIG-IP systems using the Configuration utility
K14783: Overview of the Client SSL profile (11.x – 17.x)
K14806: Overview of the Server SSL profile (11.x – 17.x)
K15462: Managing SSL certificates for BIG-IP systems using tmsh
K15497: Configuring a secure password policy for the BIG-IP system (11.x – 16.x)
K15664: Overview of BIG-IP device certificates (11.x – 16.x)
K42531434: Replacing the Configuration utility's self-signed SSL certificate with a CA-signed SSL certificate
K48615077: BIG-IP Daemons (15.x – 16.x)
K5532: Configuring the level of information logged for Traffic Management-related events
K6068: Configuring a pre-login or post-login message banner for the BIG-IP or Enterprise Manager system
K7683: Connecting a serial terminal to a BIG-IP system
K7752: Licensing the BIG-IP system
K8021: Configuring the BIG-IP LTM system to allow outbound FTP sessions
K80425458: Modifying the list of ciphers and MAC algorithms used by the SSH service on the BIG-IP system or BIG-IQ system
K9908: Configuring an automatic logout for idle sessions
K75106155: Configuring OCSP stapling (13.x – 16.x)
F5 SSL Orchestrator Deployment Guide - Version 9
Hotfix-BIGIP-16.1.3.1.0.128.11-ENG.readme
Traffic Management Shell (tmsh) Reference Guide (versions 17.0.0 and 12.0.0[1])
Platform-specific References – Hardware and vCMP
Platform Guide: i2000/i4000 Series
Platform Guide: i5000/i7000/i10000/i11000 Series
Platform Guide: i15000 Series
Platform Guide: VIPRION® 2200
Platform Guide: VIPRION® 4400 Series
vCMP for Appliance Models: Administration
vCMP for VIPRION Systems: Administration

Table 1: References

Versions of the guidance documentation referenced in this document are available on the askF5.com website; however, those may have been updated since this document was finalized. For the exact versions referenced in this evaluation, download the ISO file referenced in ***K76615426: Common Criteria Certification for BIG-IP 16.1.3.1***.

Both of the F5 sites askF5.com (resolves to https://support.f5.com/csp/home) and https://downloads.f5.com are secure sites. This is indicated by the "security padlock" icon in the browser status bar or the address bar. If

[1] The tmsh reference guide version 17.0.0 zipfile contains the pages for each of the tmsh commands. The 12.0.0 pdf contains additional general information that is still valid in 16.1.3.1 but not reproduced in the 17.0.0 zipfile.

the “security padlock” icon is not visible in the browser status bar or the address bar, you may not be connected to the correct site. As an additional precaution, check that the URL indicates that you are at f5.com. If you are unable to reach the secure F5 support site, contact F5 Support to report this problem.
Finally, you can check the fingerprint on the certificate. The correct value for askf5.com is:
SHA1 Fingerprint: 03:68:8D:19:ED:BE:50:AC:4D:F9:83:E4:57:7B:15:32:57:64:F4:1C
SHA-256 Fingerprint:
C0:4D:00:AD:1B:12:69:44:D2:78:63:0D:E3:45:2E:78:A7:83:EC:83:97:A3:FD:54:B2:B6:89:95:A4:AA:C3:67

The correct value for downloads.f5.com is:
SHA1 Fingerprint: D1:C4:69:29:1D:19:51:75:9F:DB:C6:C6:9D:93:B6:D3:35:9A:A0:CD
SHA-256 Fingerprint:
55:2D:FF:67:E4:DC:B9:2F:D9:8C:2B:14:A0:29:92:DF:19:9B:92:58:EA:5B:DE:95:55:9E:7B:93:01:2C:BB:94

Note: Additionally, the customer must login to access the product and documentation ISO downloads on the https://downloads.f5.com site.

1.2 Evaluation Scope

1.2.1 Platforms in the Evaluated Configuration

This document covers the following product evaluated against the NDcPP v2.2e + STIP PPM v1.1:

- BIG-IP version 16.1.3.1 including SSLO version 9.3, consisting of the base TMOS plus LTM (Local Traffic Manager) and SSLO (SSL Orchestrator) modules, with Appliance Mode.

This software product was tested and evaluated on the following hardware platforms. See the sections below for details on the SKUs and part numbers.

1.2.2 Hardware Platforms

Explanation of table columns in the table below.

SKU (stock-keeping unit). A set of product SKUs define the hardware and software that is licensed and shipped.

Each row in this table is a delivery option consisting of multiple product SKUs. The SKUs together define the following for appliances:

- Base BIG-IP and platform (F5-BIG-LTM-nnn)
- Additional modules (F5-ADD-BIG-SSLO-nnn)
- Appliance mode (F5-ADD-BIG-MODE).

VIPRION devices are the same, but with the addition of VPR to the SKU, and the addition of a SKU specifying the chassis (for example F5-VPR-LTM-C2400-AC).

vCMP?. A “Y” entry in the column notes that the platform supports, and the licensing allows, the use of vCMP.

Part #. This refers to the part number of the hardware device (appliance, blade, and/or chassis) included in the platform SKU.

Model Series. Designates the family of appliances or blades to which the specified SKU belongs.

SKU	VCMP?	Part #	Model Series
F5-BIG-LTM-I4600 F5-ADD-BIG-SSLO-2 F5-ADD-BIG-MODE	N	200-0390-07	i4000
F5-BIG-LTM-I5600 F5-ADD-BIG-SSLO-3 F5-ADD-BIG-MODE	N	200-0396-09	i5000
F5-BIG-LTM-I7600 F5-ADD-BIG-SSLO-3 F5-ADD-BIG-MODE	N	500-0031-01	i7000
F5-BIG-LTM-I10600 F5-ADD-BIG-SSLO-4 F5-ADD-BIG-MODE	N	500-0030-01	i10000
F5-BIG-LTM-I11600-DS F5-ADD-BIG-SSLO-4 F5-ADD-BIG-MODE	Y	500-0015-05	i11000-DS
F5-BIG-LTM-I15600 F5-ADD-BIG-SSLO-5 F5-ADD-BIG-MODE	N	500-0042-00	i15000
F5-BIG-LTM-I4800 F5-ADD-BIG-SSLO-2 F5-ADD-BIG-MODE	N	200-0390-07	i4000
F5-BIG-LTM-I5800 F5-ADD-BIG-SSLO-23 F5-ADD-BIG-MODE	Y	200-0396-09	i5000
F5-BIG-LTM-I5820-DF F5-ADD-BIG-SSLO-3 F5-ADD-BIG-MODE	Y	500-0017-17	i5000
F5-BIG-LTM-I7800 F5-ADD-BIG-SSLO-3 F5-ADD-BIG-MODE	Y	500-0031-01	i7000

SKU	VCMP?	Part #	Model Series
F5-BIG-LTM-I7820-DF F5-ADD-BIG-SSLO-3 F5-ADD-BIG-MODE	Y	500-0032-01	i7000
F5-BIG-LTM-I10800 F5-ADD-BIG-SSLO-4 F5-ADD-BIG-MODE	Y	500-0030-01	i10000
F5-BIG-LTM-I11800-DS F5-ADD-BIG-SSLO-4 F5-ADD-BIG-MODE	Y	500-0015-05	i11000-DS
F5-BIG-LTM-I15800 F5-ADD-BIG-SSLO-5 F5-ADD-BIG-MODE	Y	500-0042-00	i15000
F5-BIG-LTM-I15820-DF F5-ADD-BIG-SSLO-5 F5-ADD-BIG-MODE	Y	500-0043-00	I15000-DF
F5-VPR-LTM-C2400-AC F5-VPR-LTM-B2250 F5-ADD-VPR-SSLOC2X00 F5-ADD-BIG-MODE F5-ADD-VPR-VCMP-2400	Y	400-0028-12 400-0039-03	C2400 B2250
F5-VPR-LTM-C4480-AC F5-VPR-LTM-B4450 F5-ADD-VPR-SSLOC44X0 F5-ADD-BIG-MODE F5-ADD-VPR-VCMP-4480	Y	400-0033-04 400-0053-11	C4480 B4450

Table 2: Platform SKUs for BIG-IP including SSLO hardware platforms

1.2.3 Other Components of the Operational Environment

In addition to the BIG-IP software and hardware listed above, certain other servers (e.g. syslog for audit) are recommended or required for the operational environment.

1.2.4 Items Excluded from the Target of Evaluation via Guidance

The following items are excluded from the Target of Evaluation and **must not** be configured in order to maintain compliance with the Common Criteria evaluated configuration.

1. LBH (LOP+BUC: Lights Out Processor + Backplane Microcontroller).
   - By default, this is not accessible from the management network and guidance is not given for configuration.

2. Remote server configuration. Do not configure (do leave configuration fields blank for) these servers.
   - SNMP
   - Kerberos Delegation
   - RADIUS
   - TACACS+
3. Profiles. As with remote servers, do not configure these profiles.
   - HTTP: Web Acceleration
   - Other Application Layer Profiles: RTSP, ICAP, Request Adapt, Response Adapt, Diameter, RADIUS, SIP, Rewrite
   - Content: No profiles in this group are excluded
   - Session Persistence: Microsoft Remote Desktop Protocol, SIP
   - Protocol: SCTPß
   - SSL: No profiles in this group are excluded
   - Remote Server Authentication: RADIUS, TACACS+, CRLDP, Kerberos Delegation
   - Other: NTLM, Stream
4. IMI shell.
   - A limited usage shell is not required to configure a Common Criteria-compliant system.
5. Selected tmsh commands are not included or not allowed in the evaluated configuration. Refer to Appendix: Disallowed tmsh Commands for a list of the disallowed commands. This list also applies to iControl Rest APIs.
6. Selected iControl API modules and module interfaces are not included or not allowed in the evaluated configuration. Refer to Appendix: Disallowed iControl APIs for a list of the disallowed iControl APIs.
7. iRulesLX. iRulesLX must not be used in the evaluated configuration.
8. iAppsLX. Only iApps provided by F5 may be used in the evaluated configuration.
9. BIG-IP must not be run in debug mode in the evaluated configuration.
10. When creating support files such as QKview or TCPDUMP, the files should be immediately downloaded and deleted from the BIG-IP.
11. Do not use the ssh-agent program on the BIG-IP.

1.2.5 Security Functionality Evaluated

The following security functions were assessed and tested during the CC evaluation:

- Security Audit
- Cryptographic Support

- Identification and Authentication
- Security Management across the following interfaces:
    - Configuration utility
    - Traffic Management Shell (tmsh)
    - iControl API
    - iControl REST API
- Protection of the TSF
- TOE Access
- Trusted Path/Channels
- User Data Protection

1.3 A Note About Terminology

This document, as well as other published documentation, uses the terms Common-Criteria-compliant configuration, Common Criteria db variable, and ccmode command. You may also see the term “ccmode” (without reference to the command), although that usage is an ambiguous shorthand that is not well-defined.

Common-Criteria-compliant configuration refers to the software configuration that results from following the instructions in this Guide. It is designed to meet the claims described in the Security Target.

Common Criteria db variable is a specific configuration database variable, Security. CommonCriteria, which serves as a trigger for certain internal processing specific to Common Criteria such as always running sys-icheck at initialization or running the OpenSSL integrity tests. This variable is set by the ccmode command. It is NOT recommended that you turn off this variable. First, it does NOT back out any of the configuration changes made by the ccmode command or any manual changes made by following this document, and second, the running system which results will not be completely Common-Criteria-compliant.

ccmode command operations are described in detail in an appendix to this document; it is simply a script which includes commands to make configuring the system for Common Criteria easier. By itself it does not guarantee a compliant system. There is currently no supported way to “undo” running the ccmode script without re-initializing the system from scratch, although an advanced user could review the script and undo each command manually.

2 Installation and Configuration Procedures

The following sections provide Preparative Guidance, including installation and configuration, for BIG-IP. Administrators must review this document and all referenced documents (as necessary) before proceeding with the installation, configuration, and administration of the BIG-IP.

Versions of the guidance documentation referenced in this document are available on the askF5.com website; however, those may have been updated since this document was finalized. For the exact versions referenced in this evaluation, download the ISO file referenced in ***K76615426: Common Criteria Certification for BIG-IP 16.1.3.1***.

Note that the instructions for installation and configuration are described for one of the two boxes in the redundant-pair failover configuration. These instructions must be repeated for the second box.

2.1 Preparing for BIG-IP Installation and Configuration

- The TOE, including the BIG-IP hardware, must be installed in a secure location that provides physical protection and is not subject to physical attacks that comprise the security and/or interfere with the device's physical interconnections and correct operation. The level of security provided must be commensurate with customer policy for IT Environment secured assets.
- No general-purpose computing software will be available on the BIG-IP system, other than those services necessary for the operation, administration, and support of the TOE.
- Authorized administrative users of BIG-IP must be trusted and act in the best interest of security for the organization. This includes being appropriately trained (including security awareness training), following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
- The Administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
- The BIG-IP firmware and software is assumed to be updated by an authorized administrative user on a regular basis in response to the release of product updates due to known vulnerabilities.
- The BIG-IP must display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the TOE.
- Ensure that the components required for the operational environment are available and configured or ready to be configured. See Section 1.2.3 Other Components of the Operational Environment for details of the operational environment.
- Ensure that the BIG-IP can be configured to connect to at least three separate networks:
    - Management, for administrative functions, remote logging, and syslog communications;
        - The Management network must be a private, separate physical network that is protected from attacks and from unauthorized physical access.
    - Internal, for access to support backend servers;
    - External, for Wide Area Network (Internet) access;
    - Optional private failover network (or just a failover cable) used to separate failover connections (note that failover is not part of the evaluated functionality per the Protection Profile); and

  - If Kerberos, OCSP, AD, and/or LDAP are used (they are not part of the evaluated configuration per the Protection Profile), they also have to be on a protected network, such as the Management network.
- Ensure that the BIG-IP is configured to receive, store, and protect the audit records generated by the TOE. The BIG-IP provides audit analysis through the GUI and tmsh.
- Systems that are configured in a device group to synchronize configuration data between each other for a potential failover must be trustworthy . That means that they are all under the same administration as the TOE, identically configured and that the same assumptions can be made about them as for the TOE.
- Configuration required to meet the compliance requirements for cryptographic ciphers and algorithms are accomplished through a combination of:
  - Internal run-time processing based on the system recognizing Common Criteria mode
  - Commands run in the ccmode utility
  - Explicit configuration described in later sections of this document.
- It is assumed that digital certificates, certificate revocation lists (CRLs) used for certificate validation and private and public keys used for SSH client authentication are generated externally, meeting the corresponding standards and providing sufficient security strength through the use of appropriate key lengths and message digest algorithms. It is also assumed that Administrators verify the integrity and authenticity of digital certificates and key material before importing them into the TOE, and verifying that certificates are signed using Protection Profile-compliant hash algorithms as defined in the Security Target.
- The BIG-IP automatically performs several self-tests on each startup of the system.
  - The BIOS Power-On Self-Test is a diagnostic program that checks the basic components required for the hardware to function. It is run only at power-on. Failures display on the console; call F5 Support if any of the BIOS POST tests fail.
  - The sys-icheck utility provides software integrity testing by comparing the current state of files in the system with a database created at install time and reports all discrepancies. This is run automatically by the ccmode utility and at each system boot, and can be run from the tmsh shell on demand. The sys-eicheck.py utility provides HMAC integrity testing. When a discrepancy is detected, the utility reports that discrepancy. The utility can be run at any time during system operation, and will just report errors. In addition, the HMAC integrity test is executed during every reboot and will halt the boot if errors are found.
  - OpenSSL, cryptographic algorithm, and random number generation tests are run at boot time. They will halt the boot if failure occurs, and the administrator should reinstall.
- The Administrative-users must ensure that networking equipment is discarded or removed from operation in a manner that ensures that unauthorized access to the sensitive residual information previously stored on the equipment is not possible. This includes ensuring that cryptographic keys, keying material, PINS, and passwords on network devices are not accessible after the devices are discarded or removed from operation.
- By default, BIG-IP implements key destruction using an approved cryptographic key destruction method.
- The cryptographic operations in BIG-IP are configured at the protocol level, via the ccmode utility, and via instructions in this guide.
- The random number generator implemented in BIG-IP does not require configuration because the entropy sources are securely configured by default.

2.1.1.1 Documentation

The download site for the Common Criteria-certified release also publishes an ISO containing an archive of the referenced product documentation, CommonCriteriaDocumentationSSLO-16.1.3.1.iso. The file CommonCriteriaDocumentationSSLO-16.1.3.1.sha256 contains the SHA256 hash of the file for verification.

2.1.1.2 Establishing Administrative Access

The BIG-IP can be configured using any one or a combination of the following interfaces across either a local (direct ethernet) or remote (over the management network) connection to the TOE:

- Traffic management shell (tmsh) over SSH
- Web GUI over HTTPS
- iControl SOAP or iControl REST (both programmatic interfaces) over TLS.

This guide provides instructions for initial configuration using TMSH; customers more familiar with the web GUI can use the related web GUI functions instead. For additional configuration, any of the four interfaces may be used subject to the restrictions in section 1.2.4 Items Excluded from the Target of Evaluation via Guidance.

Refer to the *Platform Properties* section of the ***BIG-IP System Essentials*** manual for details on setting up the BIG-IP management port access.

2.2 Perform Basic Installation and Configuration

2.2.1 General Notes on Installation

2.2.1.1 Hardware and vCMP

BIG-IP hardware devices are shipped directly from the manufacturer via trusted carrier (generally FedEx) and tracked by that carrier. The sealed box includes a packing slip with a list of the components inside, and with labels outside printed with the product nomenclature, applicable sales order number, and product serial number.

When receiving a BIG-IP hardware device, inspect the packaging for tampering or other issues, that the external labels match the expected delivery and the internal product, and that the components in the box match those on the documentation shipped with the product.

It is assumed that there is a version of the BIG-IP software installed on the BIG-IP hardware. However, to ensure that the system about to be configured for Common Criteria has not been tampered with, you must download the release image and any required hotfixes and install it.

If you are unfamiliar with the process of installing BIG-IP releases, start with the descriptions of the *install* and *image* commands in the ***Traffic Management Shell (tmsh) Reference***. These commands address installing and managing images as well as how to create a new volume if required.

In general, you need to have an inactive boot volume on which to install the image, and you need to have downloaded the release ISO and its associated signature files for verification.

2.2.1.2 Verifying the Installed / Running Versions of the Software

To verify the versions of the BIG-IP software installed on the box and active, use either the GUI or tmsh commands on the active system as described below. To verify that the correct (evaluated) version has been installed, compare the version on the active slot with the version specified in section 2.2.2 Re-install the BIG-IP software.

The **tmsh show sys software status** command produces output like this, showing the two slots on the box (for a hardware installation) and what software is installed on each slot. Note that slot 1 in the example below shows the version of the TOE being certified; slot 2 shows the version of another build; there are no restrictions on the build that can be installed in that second slot.

```
------------------------------------------------------------
Sys::Software Status
Volume   Product   Version    Build  Active    Status
------------------------------------------------------------
HD1.1     BIG-IP   16.1.3.1  0.0.11     yes  complete
HD1.2     BIG-IP   14.10.03  0.75.6      no  complete
```

The GUI page **System -> Software Management: Image List** displays a similar table.

To verify the version of the BIG-IP software on the second box in the redundant configuration, the same command must be run on that box.

Refer to the ***Traffic Management Shell (tmsh) Reference*** for more information.

2.2.2 Re-install the BIG-IP software

To install a clean version of the 16.1.3.1 system, download a new copy of the software at the version 16.1.x level from the F5 download site (https://downloads.f5.com) and verify it. For a hardware or vCMP installation, it is recommended to install the clean version on an inactive boot drive.

Since the exact look of the F5 Downloads site may change over time, the instructions below for what to download are specific as to files but otherwise don’t provide detailed instructions for navigating the site. The following guidelines remain valid, however:

- Look for a link or pulldown to access downloads for v16.x.
- Once there, choose 16.1.x
- The page that comes up has links to pages for all of the 16.1.x product and related files.
- Look for “16.1.3.1, and choose that.
    - “16.1.3.1” contains the following:
        - Release notes
        - Public keys for digital signature verification of ISO image filesets
        - Product ISO
        - Digital signature files associated with the product ISO
        - Engineering hotfix files for all updates

Perform the following steps to install a clean version of 16.1.3.1.

2.2.2.1.1 Hardware and vCMP

1. Download version 16.1.3.1 and the EHF
    a. BIGIP-16.1.3.1-0.0.11.iso
    b. BIGIP-16.1.3.1-0.0.11.iso.sig OR BIGIP-16.1.3.1-0.0.11.iso.384.sig
    c. Hotfix-BIGIP-16.1.3.1.0.128.11-ENG.iso
    d. EHF sig file – Hotfix-BIGIP-16.1.3.1.0.128.11-ENG.iso.384.sig or Hotfix-BIGIP-16.1.3.1.0.128.11-ENG.iso.sig
    e. archive.pubkey.20130729.pem (for the iso.sig files) OR archive.pubkey.20160210.pem (for the iso.384.sig files)
2. Verify the images using the signature file and public key (see section 2.2.2.2 Verifying the product ISO using the digital signature for details).
3. Install the 16.1.3.1 software.
4. Install the EHF. For details, see ***K13123: Managing BIG-IP product hotfixes (11.x – 17.x)***.

2.2.2.2 Verifying the product ISO using the digital signature

Along with the .iso file or image fileset that contains the product software, the download site includes several other files, the important ones being: *.pem, *.sig, and *.384.sig. The *.pem file contains the public key needed for the verification step below. The *.sig and *.384.sig files contain a digital signature, and are used to verify that the ISO or image fileset you download is the one F5 produced. Either the *.sig or *.384.sig may be used for hardware and vCMP; *.384.sig must be used for image filesets.

When the signature verification feature is enabled, the digital signature is used to verify the ISO as part of the download. This feature is always enabled when the Security.CommonCriteria DB variable is ON. The ccmode command sets the Security.CommonCriteria DB variable to ON so this feature is enabled in the evaluated configuration.

If the signature verification on the BIG-IP fails, the software update installation will fail. In this case, try to download the ISO again. If the signature verification fails a second time, contact F5 Support.

To verify the ISO before the ccmode command is run, use third party tools such as the openssl utility on the system to which you’ve downloaded the ISO, .sig or .384.sig, and .pem files.

Examples of these on a Linux system is:
Product ISO:

```
openssl sha256 –verify archive.pubkey.20130729.pem –signature BIGIP-16.1.3.1-0.0.11.iso.sig BIGIP-16.1.3.1-0.0.11.iso
```

An equivalent example on Windows is:
Base ISO:

```
C:\Users\fred\Desktop>openssl dgst -sha256 -verify
archive.pubkey.20130729.pem  -signature BIGIP-16.1.3.1-0.0.11.iso.sig  BIGIP-
16.1.3.1-0.0.11.iso
```

If the signature verification fails (the openssl command gives a "Verification Failed" error message), the software update installation will fail. In this case, try to download the ISO again. If the signature verification fails a second time, contact F5 Support.

2.2.2.3 Updating BIG-IP software after initial configuration

For hardware and vCMP, the process of updating BIG-IP is the same as the initial install, except the administrator does not need to verify the image. Since the ccmode command has already been run during the initial install, the BIG-IP will automatically verify the new ISO using the digital signature as part of the upload and installation process initiated by the administrative-user. (For additional information, refer to *About Liveinstall signature checking in ccmode* in ***BIG-IP System: Essentials***.) If the signature verification fails, the software update installation will fail. In this case, try to download the ISO again. If the signature verification fails a second time, contact F5 Support.

2.2.3 SSH Configuration

An update to SSH configuration must be performed before applying the Appliance Mode license: public-key configuration and SSH cipher algorithms.

2.2.3.1 Using SSH public-key authentication

If you plan to use public-key-based authentication for management via SSH, you must configure it before applying the Appliance Mode license. Perform the following steps:

```
mkdir /home/<username>
mkdir /home/<username>/.ssh
chgrp webusers <groupname>
vim /home/<username>/.ssh/authorized_keys
chmod 644 /home/<username>/.ssh/authorized_keys
restorecon -R -v /home/
```

where:

```
<username> is the name of the user to whom you're granting access
<groupname> is the group for the keys file
Authorized_keys contains the keys you're authorizing
```

Note that this set of commands must be executed for each user being authenticated, and that you can define the keys for users not yet defined to the BIG-IP. You may define those users later using tmsh or the GUI.

2.2.4 Setting up the banner for the serial console

The banner for the serial console must be configured before activating the BIG-IP license. Refer to ***K6068: Configuring a pre-login or post-login message banner for the BIG-IP or Enterprise Manager system*** for instructions on setting up that banner.

2.2.5 Activate the software license

In order to use the BIG-IP software, you must activate the license you received from F5. For instructions on activating the license, refer to ***K7752: Overview of licensing the BIG-IP system***.

Once the license is activated, verify that it includes the following:

- The license must include only SSLO in addition to the base LTM
- The license must include Appliance Mode.

To check the contents of the license, use the GUI and go to the System -> License page, then verify that the required components are present in the active licenses section.

2.2.6 Execute the Configuration Setup Utility

Execute the Configuration Setup utility to configure basic information such as admin password, management port IP address(es), basic network information, and high availability configuration.

2.2.6.1 High Availability (optional)

If configured, high availability must be set to an Active / Standby configuration. Active / Active is not supported. Connection mirroring must be enabled, but is not supported for SSL forward proxy connections, and configuration data must be encrypted immediately before synchronization. Note that this must be done before the ccmode command is run or the HA connection will not come up.

Note that the default HA configuration will automatically synchronize the systems, so your configuration will be automatically synced as you go through the configuration process.

Refer to the *Creating an Active-Standby Configuration Using the Setup Utility* in the ***BIG-IP Device Service Clustering: Administration***.

2.2.7 Create an Administrative User with tmsh access

Create an administrative-user with the Administrator role and tmsh access. You will perform the rest of the configuration steps logged in as this user.

Note that there is no password policy enforcement in effect at this time, but you must create the password for this administrative-user according to the policy described in section 3.1.

Refer to *Local User Account Management* in ***BIG-IP System: User Account Administration***.

NOTE: It is strongly recommended that, in addition to the administrative-user created above, you configure the primary administrative user (generally “admin”) with tmsh access as well, as this user is the only administrative-user able to login locally if otherwise locked out.

2.3 Common Criteria configuration

2.3.1 ccmode command

The ccmode command is the first step in configuring the BIG-IP to be compliant with specific Common Criteria requirements. It performs functions such as setting the required password policy, the allowed ciphersuites for TLS, logging options, etc. For a complete list, see section 4.

Perform this step by issuing this command from the tmsh command line:

```
      ccmode
```

Note that ccmode performs an integrity check on the system; this can take several minutes.

Once the ccmode command is issued, the DB variable Security.CommonCriteria is set. While this can be used as an indication that the ccmode command has been run and its settings are in effect, note that a complete Common Criteria configuration consists of licensed Appliance mode, running the ccmode command, and following the configuration instructions in this document.

Note that when the 16.1.3.1 EHF is installed, there are two errors that are expected and should be ignored:

```
      Run the sys-icheck utility: ERROR:
      S.5…….      /usr/lib/python2.7/susconfig.pyc
      ERROR: S.5…….      /usr/lib/hmac-binaries/hmac-of-binaries.db
      --- System integrity check complete:
            2 unrecoverable errors were found.
```

Refer to Section 4, **Appendix: ccmode command** (this document) for more information on *ccmode*.

2.3.2 High Availability (this step required if the optional HA feature is configured)

In order to ensure that your configurations can sync after running the ccmode command, you must issue the command

```
      tmsh modify net self-allow defaults add {tcp:443 tcp:4353}
```

The self-ips configured for the mirroring VLAN must also be allowed using the following command, replacing <name> with the name of the self-ip you configured.

```
      tmsh modify net self <name> allow-service default
```

2.3.3 Establish local users and roles

2.3.3.1 Administrative users

Configure administrative accounts, their associated roles, and password-policy-compliant passwords. Note that administrative-users are only configured locally.

Ensure that at least one administrative-user account has tmsh access, preferably one in addition to the primary administrative user. **It is strongly recommended that the primary administrative user (generally "admin") have tmsh access, as this user is the only administrative-user able to login locally if otherwise locked out.**

Refer to *Local User Account Management* in ***BIG-IP System: User Account Administration***.

For more information on user roles refer to *User Roles* in ***BIG-IP System: User Account Administration***.

2.3.3.2 Log Manager users

Create a Log manager role if desired. The Log Manager role is not listed in the 16.x BIG-IP Systems: User Account Administration, but it is listed in the 17.x version of the doc and is the same. That information is copied here:

This role grants users permission to view all configuration data on the system, similar to an Auditor role. However, users with this role can modify the system log configuration settings, including remote logging, log filters, destinations, and publishers. These users can change their own user account password but cannot change their partition access. When granted terminal access, a user with this role has access to TMSH but not the advanced shell.

System log configuration options, including remote logging, log filters, destinations, and publishers.

If a user is assigned as Log Manager, they may not be assigned to any other roles.

2.3.4 Login to the BIG-IP

Review the article ***K13092: Overview of securing access to the BIG-IP system*** for an overview of the methods to control and manage user roles, authentication, and passwords.

2.3.4.1 SSH

To login to the BIG-IP via SSH, use an SSH client to establish a session to the IP address configured during installation and initial setup. Login via an administrative-user account with tmsh access, using the userid and password established in section 2.3.3.1 Administrative users.

If you wish to use public key SSH host-based authentication, see the section on one way secure shell host-based authentication from a remote system to the BIG-IP system in ***K13454: Configuring SSH public key authentication on BIG-IP systems (11.x - 16.x)*** for setup and usage instructions.

2.3.4.2 GUI

To login to the BIG-IP via the GUI, access the IP address configured during installation and initial setup through a web browser via HTTPS, and enter the userid and password of an established administrative-user on the login screen.
If you have not configured an SSL certificate to replace the configuration utility (GUI)'s self-signed certificate, you may still access the login screen by making a single security exception, but the browser will show the connection as insecure. To replace the self-signed certificate, see ***K42531434: Replacing the Configuration utility's self-signed SSL certificate with a CA-signed SSL certificate.***

2.3.5 Login welcome banners

Common Criteria compliance requires that an advisory notice and consent warning be displayed before establishment of any interactive administrative user session. The warning is defined by an authorized

administrator; Common Criteria does not specify the wording. However, something like the following would be appropriate:
"Welcome to the BIG-IP. Unauthorized use of this system is prohibited."

For the BIG-IP, this notice must be displayed for GUI and tmsh sessions.

Configuring security settings for administrative login
Use this procedure to define: the maximum number of concurrent users allowed, the maximum duration that the Configuration utility can be idle before automatic user logout, and a security message that you want the system to display on the BIG-IP Configuration login screen.

1. On the Main tab, click **System** > **Preferences**.
2. From the **System Settings** list, select **Advanced.** Additional settings appear on the screen.
3. In the field labeled **Maximum HTTP Connections To Configuration Utility**, retain or revise the default value.
4. In the field labeled **Idle Time Before Automatic Logout**, revise the default value. F5 recommends a value of 120 seconds.
5. For the setting labeled **Show The Security Banner On The Login Screen**, verify that the box is checked. This ensures that security message you specify displays on the login screen of the BIG-IP Configuration utility.
6. In the field labeled **Security Banner Text To Show On The Login Screen**, revise the default security message. A good security message is one that provides legal protection to the organization, such as a message stating that unauthorized access is forbidden. The login screen of the BIG-IP Configuration utility displays the text that you specify in this field.
7. Click **Update**.

To configure this feature from the command line refer to the *sys sshd* section in the ***Traffic Management Shell (tmsh) Reference***.

2.3.5.1 GUI

The GUI warning message is enabled by default, and defaults to "Welcome to the BIG-IP Configuration Utility." To update that message and ensure that it is enabled, use the following command from within tmsh, replacing **<Text>** with your desired text.

```
modify sys global-settings gui-security-banner enabled gui-security-
banner-text "<Text>"
```

Refer to the *sys sshd* section in the ***Traffic Management Shell (tmsh) Reference***.

2.3.5.2 Tmsh

The warning banner for tmsh is disabled by default, and so the following command must be run to enable it and define the message, replacing **<Text>** with your desired text.

```
modify sys sshd banner enabled banner-text "<Text>"
```

Also see the *sys sshd* section in the ***Traffic Management Shell (tmsh) Reference***.

2.3.6 VLAN settings

When configuring VLANs, ensure that the "Source Check" and "Fail-safe" options are enabled. The "Fail-safe Timeout" value must be at least the default value, and "Fail-over" is the action the BIG-IP must take when the timeout expires.
Network:VLANs: each one
You must drop down the "Configuration: Advanced button to see the fail safe button.

Refer to the *Creating an Active-Standby Configuration Using the Setup Utility* in the ***BIG-IP Device Service Clustering: Adminstration***.

Refer to *VLANs, VLAN Groups, and VXLAN* in ***BIG-IP TMOS: Routing Administration***.

2.3.7 Packet Filtering

2.3.7.1 Packet Filtering

Basic packet filtering functions are available. If you choose to enable and configure basic packet filtering, configure the BIG-IP to fail closed.

To do this, configure the ***Unhandled Packet Action*** property to either **Discard** or **Reject**.

In the GUI, this property is on the page Network -> Packet Filters: General. Note that it only appears if Packet Filtering is enabled.

Warning: Changing the default value of the Unhandled Packet Action property can produce unwanted consequences. Before changing this value to Discard or Reject, make sure that any traffic that you want the BIG-IP system to accept meets the criteria specified in your packet filter rules.

To ensure that all packets denied are also logged, create a packet filter rule to deny traffic and enable logging. Instructions for this are in the Packet Filters section of the ***BIG-IP TMOS: Routing Administration***.

Refer to the ***tmsh Reference Guide*** and ***BIG-IP TMOS: Routing Administration*** for details on configuring packet filtering.

2.3.8 Event (audit) logging

The Common Criteria-compliant logging configuration has several requirements and behaviors:

1. Certain logging options must be set so that the BIG-IP generates the required event records. The following must be enabled:
   - Local Traffic Logging: MCP = Notice
   - Local Traffic Logging: Traffic Management OS = Notice
   - Audit Logging: MCP = Enable
   - Audit Logging: tmsh = Enable
   - If Packet filtering is enabled, then the logging option for each rule must be enabled. Refer to the ***tmsh Reference Guide*** and ***BIG-IP TMOS: Routing Administration*** for details on configuring packet filtering. Also refer to section 2.3.7.1 for configuring logging for the default deny policy.

2. BIG-IP protects the local audit trail from unauthorized modification and deletion with no action required by design; no action is required on behalf of the administrator.
3. Logging must be configured to use a dedicated network interface. This ensures a limited attack surface for the administratively-controlled logging function. See section 2.3.8.1 Configuring a dedicated network interface for details on configuring this interface.
4. Secure remote logging of event records, and local logging as a backup in case the remote connection fails, are required. The logging framework will simultaneously send the event record to both of the subscribed (remote and local) recipients. Refer to *Configuring Remote High-Speed Logging* in ***External Monitoring of BIG-IP Systems: Implementations*** for details on configuring secure remote logging with local logging as a backup.
   Note that when configuring the Server SSL profile for the connection path to the syslog server, the Authenticate Name can be configured as an IPv4 address. The TOE supports both CN and the SAN extension. Refer to the description of "Authenticate Name" in ***K14806: Overview of the Server SSL profile (11.x – 16.x)*** for details on configuring that option.
5. A warning is issued when 90% of local log storage is full; this warning is logged in the log files.
6. Should the connection between the BIG-IP and syslog server fail, the BIG-IP will retry the connection an unlimited number of times until the connection can be re-established. During this time, log records will continue to be logged locally.
7. The BIG-IP system implements an authentication cache for all configuration utility requests (iControl SOAP, iControl REST). When a successful configuration request occurs, information is stored in the cache and a cookie sent to the client; the cookie is authenticated against the cache on subsequent requests. Note that authentication logging is NOT performed on all cookie authentication requests; it is performed on the first authentication, on any failure, and on the next successful connection attempt after cookie expiration or cache invalidation.

2.3.8.1 Configuring a dedicated network interface

The following steps are required to create a dedicated network interface for logging:

1. Create a dedicated VLAN for logging
2. Assign a dataplane interface to the VLAN
3. Assign one or more static self-IPs to the interface (several self-IPs help prevent source port exhaustion).
4. Ensure that the remote syslog pool of servers created as described in section 2.3.8 Event (audit) logging is configured to be on the dedicated VLAN.

For information on configuring VLANs and assigning interfaces and self-IPS to them, refer to *VLANs, VLAN Groups, and VXLAN* in ***BIG-IP TMOS: Routing Administration***.
For more information on self-IPs, refer to *Self IP Addresses* in ***BIG-IP TMOS: Routing Administration***.

2.3.8.2 Configuring fault_monitor

The ccmode script starts fault_monitord when BIG-IP is common criteria enabled.

fault_monitord monitors availability of local audit storage by periodically checking for used disk space in the log volume against a configurable threshold. If the used disk space exceeds the threshold, fault_monitord recognizes the status of local audit storage as down.

fault_monitord also monitors availability of remote audit storage when configured. The external audit server is defined in a pool as a pool member. The pool has a health monitor enabled to check for availability of this pool member. When configured, fault_monitord will periodically check the availability status of this pool. If the pool goes offline, fault_monitord recognizes the status of remote audit storage as down.

If neither local audit storage nor remote audit storage is up, fault_monitord enters the BIG-IP system into degraded mode. The fault monitor daemon will stop TMM with **bigstart stop tmm**. The audit systems can then be fixed, and the device rebooted.

The following commands can be used to configure fault_monitor.

Command	Description
tmsh restart sys service fault_monitord	Restart fault_monitord
tmsh show sys service fault_monitord	Check fault_monitord running status
tmsh mod sys db log.fault_monitord.level value "<value>" **setdb log.fault_monitord.level "<value>"** **tmsh list sys db log.fault_monitord.level** **getdb log.fault_monitord.level**	Set and get logging level
tmsh mod sys db fault_monitord.disk_check.Interval value "<value>" **setdb fault_monitord.disk_check.Interval "<value>"** **tmsh list sys db fault_monitord.disk_check.Interval** **getdb fault_monitord.disk_check.Interval**	Set and get timer interval
tmsh mod sys db fault_monitord.disk_check.Threshold value "<value>" **setdb fault_monitord.disk_check.Thresholdl "<value>"** **tmsh list sys db fault_monitord.disk_check.Threshold** **getdb fault_monitord.disk_check.Threshold**	Set and get disk threshold

Table 3: fault_monitor commands

BIG-IP logs a warning if the local space for syslog files on the box exceeds a configurable maximum size. The TOE implements a local syslog file rotation scheme that numbers the locally archived syslog files. The TOE will delete the oldest syslog file once the maximum size for local syslog file space is exceeded. A cron job runs every two minutes to check the audit trail storage partition in order to accomplish this. The evaluated configuration requires allocation of 7 GB of audit storage, and a warning to be logged when 90% of the storage space is exhausted. The administrator receives the warnings when reviewing the log files.

2.3.9 Certificate Management

For information on certificates and certificate management, see the following:

- Device certificate overview: ***K15664: Overview of BIG-IP Device Certificates***
- SSL certificate management: *SSL Certificate Management* section of ***BIG-IP System: SSL Administration*** The same document contains sections on creating and requesting certificates, SSL traffic management, and configuring client- and server-side traffic.
- Certificate management through the GUI: ***K14620: Managing SSL certificates for BIG-IP systems using the Configuration utility***
- Certificate management through tmsh: ***K15462: Managing SSL certificates for BIG-IP systems using tmsh***

To ensure that the revocation of intermediate certificates causes a connection to fail, the intermediate CAs must NOT be in **Trusted Certificate Authorities**. BIG-IP considers all Intermediate certificates which were set in **Trusted Certificate Authorities** as trusted anchors which are not validated (they are explicitly trusted), so it cannot be revoked. Therefore, when configuring your SSL profile, follow the instructions in ***K14806: Overview of the Server SSL profile (11.x – 16.x), K14783: Overview of the Client SSL profile (11.x – 16.x),*** and ***K13302: Configuring the BIG-IP system to use an SSL chain certificate (11.x – 16.x)*** to define only the root CA as the trust anchor.

2.3.10 Restricting Ciphers

For the list of allowable ciphersuites for TLS and SSH, see section 5 Appendix: Allowed Ciphersuites for TLS and SSH.

2.3.10.1 SSL Profiles

The ccmode command sets the allowable ciphersuites for the default client and server SSL profiles: clientssl and serverssl.

Create and use SSL profiles based only off those default profiles, and do not modify the configured ciphersuites, in order to ensure that your TLS connections are Common-Criteria-compliant.

Do not use the ssl-insecure-compatible and serverssl-insecure-compatible default profiles, as these include weak TLS ciphers which are not Common-Criteria-compliant.

When configuring SSL profiles, only use 2048-bit or higher RSA key sizes, or ECDSA curves p-256 or p-384.

Refer to *ltm profile server-ssl* in the ***Traffic Management Shell (tmsh) Reference***.

2.3.10.2 SSH

The ccmode command and the default SSH server profile set the allowable ciphersuites for SSH.

The default rekey limit set in the SSH configuration file provided with the BIG-IP ensures that not more than 2^28 packets are transmitted or 1 hour passes before the session keys are rekeyed. Session key rekeying will occur when the first of these thresholds is reached.

If the default rekey limit must be changed, edit the SSH configuration to change the data, time, or both parameters using a command similar to the following, where “512M” and “1800s” are the data and time parameters, respectively:

```
    tmsh modify sys sshd include ‘RekeyLimit 512M 1800s’
```

2.3.11 System Time Configuration

Refer to the *sys clock* command in the ***Traffic Management Shell (tmsh) Reference*** for details on setting the system time.

Refer to *General Configuration Properties* in ***BIG-IP System: Essentials***.

2.3.12 Session Inactivity Termination

BIG-IP terminates local and remote interactive administrative user sessions (Console, Configuration Utility or tmsh) after an administrator-defined period of inactivity.

Refer to ***K9908: Configuring an automatic logout for idle sessions*** for details on configuring these timeouts. Note that the ccmode script sets the tmsh timeout for 20 minutes.

2.3.13 SSLO Configuration

Please see the ***F5 SSL Orchestrator Deployment Guide - Version 9***.

2.3.13.1 Certificate Enrollment

During initial system setup, the administrator must either import or generate an asymmetric key pair and CA certificate signed by a trusted external CA to the embedded CA.

The administrator can either generate a key pair and CA certificate on an external system and import the key pair and certificate, or generate a key pair on the TOE, generate a CSR, send it to an external CA to create a signed CA certificate, and import that certificate into the TOE.

The system must be configured to include a key pair and CA certificate for the embedded CA using one of these methods. This process can be repeated by an authorized administrator at any time the system is running to update or change the certificate for the embedded CA.

Refer to *SSL Certificate Management* in ***BIG-IP System: SSL Administration***.

2.3.13.2 TLS Session Establishment Policy

TLS session establishment policies can be configured as rules through the SSLO Security Policy UI. Please refer to the *Managing Security Policies* section in the ***F5 SSL Orchestrator Deployment Guide - Version 9*** for instructions on how to do this.

2.3.13.3 Ordering of Cipher Suites in the Client Hello

The cipher suites in the Client Hello are not listed in descending order of strength by default, this needs to be configured in the SSL profiles. To obtain this reordered list, within the Client SSL profile and Server SSL profile, go to **Configuration > Ciphers > Cipher Suites** and enter “cc_stip:@STRENGTH” into the Cipher Suites box. Now the cipher suites will be listed in descending order of security strength.

Optionally, the SSL profiles can be configured to list the cipher suites based on their operating speeds with the “@SPEED” command.

2.3.13.4 Connection Summary Logging

Connection summary logging is an optional feature and can be enabled if the user would like to see log messages summarizing each client/server connection.

This can be enabled in the GUI under **SSL Orchestrator > Configuration** > **Log Settings**. From there, select **Information** from the **SSL Orchestrator Generic** drop down, then select **Save & Next** then **Deploy**. Now you will see a traffic summary log message per-connection, detailing connection properties, whether it was decrypted, and which Service Chain it was sent through.

2.3.13.5 SSL Profile Configuration

The server name can be set in an SSL profile, please refer to the *Additional SSL Profile Configuration Options* section in ***BIG-IP System: SSL Administration*** for details.

Renegotiation period and time can also be configured in an SSL profile. The renegotiation period option controls the amount of time, in seconds, that the system waits before renegotiating the SSL session. The renegotiation size option controls the amount of data exchanged, in megabytes, before the system renegotiates the SSL session.

After the SSL profiles are created by SSLO, to remain in the evaluated configuration, the administrator must change the certificate lifespan to 1 day. This can be done with the following command:
modify ltm profile client-ssl <profile name> cert-lifespan 1

Refer to ***K14783: Overview of the Client SSL profile (11.x – 17.x)*** and ***K14806: Overview of the Server SSL profile (11.x – 17.x)*** for more information.

2.3.13.6 Auditing Configuration

SSLO audit records are written to /var/log/restonoded/ssloAudit.log. In order to view these records from the GUI or have them sent to remote logging, the following command must be ran to tie this log file in with the syslog system. (Please adjust the syslogIP/port as desired.)

```
tmsh modify sys syslog include 'source s_sslo_audit {
file("/var/log/restnoded/ssloAudit.log" follow_freq(1) flags(no-parse)); };
destination d_to_secure_syslog { syslog(xx.xx.xx.xx transport(udp) port(514)
); }; log { source(s_sslo_audit);destination(d_to_secure_syslog); };'
```

2.3.13.7 Consent for TLS Inspection

The ccmode script by default enables STIP mode db variable if SSL Orchestrator is licensed. The warning message is in the ccmode script and contains the following, “Running in STIP mode requires the system to intercept and inspect TLS traffic. If you do not consent, please set the 'inspectionconsent' db variable to 'no'”.

2.3.13.8 Plaintext Routing Function

The following iRule will create a new audit record with the plaintext routed to the inspection processing functional component. Attach this iRule to the virtual server(s) created by SSLO iAppLX and modify the log message itself to include additional texts as appropriate.

```
when CLIENT_ACCEPTED {
  set sid "NA"
}
when CLIENTSSL_HANDSHAKE {
  set sid [SSL::sessionid]
}
when CONNECTOR_OPEN {
  log local0. "SID $sid connector [CONNECTOR::profile]"
}
```

2.4 Synchronize the completed configuration and reboot

If the administrator configures high availability, in order to ensure that both systems of the redundant pair are correctly configured, and to maintain a secure configuration state in case of failover, the administrative-user must issue a synchronization command to synchronize the configurations. This must be done before deploying the Common Criteria-compliant systems and any time thereafter when configuration changes are made.

Once the completed configuration has been synchronized, reboot both systems. This is required so that certain defined variables can be picked up and acted upon at startup.

Refer to the *Creating an Active-Standby Configuration Using the Setup Utility* in the ***BIG-IP Device Service Clustering: Administration***.

3 Operational Procedures

The following sections provide Operational Guidance for BIG-IP.

3.1 Password Selection Requirements

Passwords in the evaluated configuration must meet the following minimum requirements:

- Minimum length of 15,
- At least one special character,
- At least one numeric character,
- At least one uppercase character
- At least one lowercase character

Passwords should be changed every 1-3 months (ccmode configures 90 days as a default). Passwords should not include a dictionary word, email address, a proper noun, a person's name, or a username. A password must not be easy to guess, such as a birthdate or the name of a pet.

3.1.1 Configuring a password policy for administrative users

Note: the ccmode command includes password policy configuration to the Common Criteria requirements (see section 4 Appendix: ccmode command for details. You may use the instructions below if you wish to make the policy more restrictive.

Use this procedure to require BIG-IP system users to create strong passwords and to specify the maximum number of BIG-IP Configuration utility login failures that the system allows before the user is denied access.

1. On the Main tab, click **System** > **Users**.
2. On the menu bar, click **Authentication**.
3. From the **Secure Password Enforcement** list, select **Enabled**. Additional settings appear on the screen.
4. For the **Minimum Length** and **Required Characters** settings, configure the default values, according to your organization's internal security requirements.
5. In the **Maximum Login Failures** field, specify a number. If the user fails to log in the specified number of times, the user is locked out of the system. Therefore, F5 recommends that you specify a value that allows for a reasonable number of login failures before user lockout.
6. Click **Update**.

Users must protect their password from unauthorized disclosure. The password must be stored securely so that it is not accessible by other users. Never provide your password to any other individual.

Password entry is obfuscated by default.

Refer to ***K15497: Configuring a secure password policy for the BIG-IP System (11.x – 16.x)***.

3.2 Maximum Failed Login Attempts

The administrator can set a parameter that specifies the maximum number of consecutive failed login attempts that can occur before a given user account will be locked out. This feature applies to all interfaces, and there is only one counter. For example, if the administrator fails to login to the CLI twice and then the Web GUI once, the maximum number of consecutive failed login attempts is reached. The default setting is 3. It is highly recommended that the default setting be retained (i.e., not changed).

If a user becomes locked out, the user account will be unlocked after an administrator-specified duration. The ccmode script sets the default to 600 seconds (10 minutes). To change this duration, issue the command:

```
tmsh modify /sys db password.unlock_time value <value in seconds>
```

The ccmode script also configures the evaluated configuration to disable the manual unlock (in favor of the timed unlock), and to allow the primary administrative user (generally “admin”) to log on from the local serial console even if the account is locked. This ensures that at least one user account is available at all times. If the primary administrative user does log in locally, its lockout counter will be reset and it will be able to log in remotely as well.

For more information on setting up the serial console, see ***K7683: Connecting a serial terminal to a BIG-IP system***.

Note that the audit record for failed login attempts specifies only the number of attempts; to determine via the log whether an administrative user has exceeded the maximum you must manually compare the number in the audit log with the configured maximum.

3.3 Audit Review

The administrator should review the audit data at least weekly. Note that the warning for exceeding the maximum log size is documented in the log files.

See Section 9 Appendix: Audit and Event Records for the list of auditable events and the format of the audit records. This section lists all auditable events and provides the format for the audit records along with a brief description of each field.

For more information see *Auditing user access* in ***BIG-IP System: User Account Administration***.

See ***K5532: Configuring the level of information logged for Traffic Management-related events***.

3.4 Terminating Interactive Sessions

Users of the BIG-IP can terminate (log out of) their interactive sessions.

When logged into the local session via tmsh, execute the *quit* command to terminate the local session and return to the system prompt. Type *logout* or *<ctrl-d>* to close the shell session.

When logged into a remote session via SSH, exit out of SSH client to terminate the SSH and tmsh session or type *quit* (to exit tmsh) then *logout* or *<ctrl-d>* to close the shell session.

When logged into a remote session via the Web GUI, click on the "Log Out" button to terminate the Web GUI session.

3.5 Commands and APIs not Allowed in the Evaluated Configuration

Due to the exclusions, certain commands and APIs are not included or not allowed to be used in the evaluated configuration. See Section 7 for the list of disallowed tmsh commands, and Section 8 for the list of disallowed iControl APIs.

Note that the GUI greys out options that are not permitted when they are explicitly disallowed because of licensing or configuration. Some GUI options do not fall under those categories, however any GUI option that corresponds to a disallowed tmsh command or iControl API is itself disallowed.

3.6 Dependencies on the Operational Environment

The servers (see section 1.2.3 for details) in the operational environment are to be kept up-to-date with the most recent security updates and administered in a secure manner.

The Common Criteria-evaluated configuration relies upon security functionality of the underlying hardware and Linux operating system (OS) to protect the private keys, certificates, and configuration files.

3.7 Management Interfaces

3.7.1 Additional Management Interfaces

After the TOE is configured and running, two additional interfaces are available for configuration management: iControl and iControl REST. Both are programmatic interfaces over HTTPS. Refer to the SDK for each for details on setting up the connection, authenticating the user, and managing the TOE.

3.7.2 Use of Management Interfaces

All administrative interfaces are designed to be used to configure the BIG-IP, and for no other purpose. In particular, they must not be used to access external web sites other than those specifically permitted by F5 documentation.

For details on how an authorized administrator can perform management functions within each management interface, please refer to the appropriate reference guide or knowledge article listed in section 1.1 References.

3.8 Certificate Validation

The TOE supports validation of X.509 digital certificates using a certificate revocation list (CRL) as specified in [RFC 5280] Section 5. Administrators create profiles which are used to define the parameters used to communicate with an external entity. These parameters include the ability to require the use of TLS and peer or mutual authentication and a definition of the certificate to use for authentication. This capability is used to create a mutually authenticated connection with the external audit server. The external audit server provides a certificate to the TOE during establishment of the TLS connection in order to authenticate the external audit server.

The TOE offers administrative interfaces for creating a private key and certificate signing request (CSR). The CSR may include the following information: public key, common name, organization, organizational unit, country, locality, state / province, country, e-mail address, subject alternative name. After the CSR is created, the administrator must export the CSR outside the TOE. Outside the scope of the TOE, the administrator provides the CSR to the CA and then the CA returns the certificate to the administrator. Using the administrative interface, the administrator can then import the certificate into the TOE.

The only method supported by the TOE for obtaining a CA certificate is for the administrator to save a certificate to a text file and import it into the TOE. The certificates are stored in a text file. The TOE is capable of importing X.509v3 certificates and certificates in the PKCS12 format. The TOE is also capable of creating and using a self-signed certificate.

The TOE checks the validity of the certificates when the profile using the certificate is loaded and when the certificate is used by the TOE, including during authentication. If the certificates are modified, the digital signature verification would detect that the certificate had been tampered with and the certificate would be invalid. Administrators can ensure that the certificates presented have not been revoked by importing a certificate revocation list (CRL) into the TOE. A certificate chain includes the root CA certificate, certificates of intermediate CAs, and the end entity certificate. The certificate chain consists of all the certificates necessary to validate the end certificate. Administrators can upload trusted device certificates (root CA certificates) into the TOE to identify which certificates are trusted. The TOE performs full certificate chain checking using Public Key Infrastructure X.509, verifies the expiration of the certificate (assuming a reliable time), and verifies its revocation using CRLs.

When the validity of a certificate cannot be established, the TOE will allow the administrator to choose whether or not to accept the certificate.

3.8.1 CA Certificate Storage

The TOE includes a file containing CA certificates (/config/ssl/ssl.crt/ca-bundle.crt). This file can be updated automatically through a BIG-IP upgrade or manually through the CA bundle manager. Refer to the section *SSL Certificate Management* in ***BIG-IP System: SSL Administration*** for instructions on how to load or remove CA certificates from the bundle.

Access control of certificate files can be configured through user account administration. A user with the role of Administrator or Certificate Manager will be granted access to certificate and key files.

3.9 Starting and Stopping Services

The Security Administrator is able to start and stop the following services using the "bigstart <stop, start, restart> <service>" command or the following tmsh command "tmsh <stop, start, restart> /sys service <service>". The list of services that can be started and stopped, and details for doing so, are found in ***K48615077: BIG-IP Daemons (15.x – 16.x)***.

3.10 Session Resumption

The TLS server supports session resumption based on session tickets according to RFC 5077. These session tickets adhere to the structural format described in Section 4 of RFC 5077. These session tickets are encrypted using the AES with CBC mode symmetric algorithm with 128 bit key length.

Session establishment creates a session ID. When a new context is started and a session ID is offered, the session ID is verified to be acceptable to allow session resumption by checking the validity of the session ID in the session ID table, the age of the session ID, the cipher suite offered in the session ID, configuration settings of the session ID, and the Server Name Indication (SNI). Any failure in these validation steps listed below would trigger a full handshake.

Multiple contexts are supported for session resumption. A session can be constructed in one context and resumed in another context. The context which constructs the session ID during full handshake is the owner of that session ID and also validates the session ID and session state. Contexts which resume a session request that the originating context session owner validate the session ID and session state. If the originating context session validation response does not validate the session, a full handshake is triggered. Contexts validate sessions by requesting that the originating owner of a session validate a session before resumption can continue. If a session is not validated, a full handshake is triggered.

3.11 SSL Forward Proxy Configuration

The SSL forward proxy functionality within the TOE allows traffic to be encrypted between a client and the TOE, using one certificate, and traffic to be encrypted between the TOE and the server, using a different certificate. The TOE intercepts all encrypted traffic then routes the data to inspection components within or external to the TOE. Refer to the section *Implementing SSL Forward Proxy on a Single BIG-IP System* in ***BIG-IP System: SSL Administration*** for additional information on how to configure these settings.

3.11.1 Certificate Repository

The SSL forward proxy in BIG-IP implements an in-memory certificate store for dynamically generated server certificates. A generated server certificate has a lifespan that either matches the expiration time in the origin server certificate or is the "Certificate Lifespan" setting, in day(s), in the attached clientSSL profile, whichever is shorter. Expired certificates are automatically purged from the in-memory certificate store. Generated certificates in this in-memory certificate store are local to this BIG-IP unit and are not synchronized to the standby device.

The certificates are stored in *certificates.log* syslog audit trail.

3.11.2 Configuring Supported Groups in the Client Hello

The following groups are supported and can be configured in the Configuration utility using Cipher Group: secp256r1, secp384r1, ffdhe2048, ffdhe3072, and ffdhe4096. Refer to ***BIG-IP Local Traffic Manager: Configuring a Custom Cipher String for SSL Negotiation*** for additional details on how to configure cipher rules and cipher groups.
When the ccmode script is run it turns on STIP mode, and the cipher group is preselected to use "f5-cc-stip" which contains the cipher suite list “cc_stip”. This should not be changed.

3.11.3 OCSP Configuration

The instructions below can be used to set up Online Certificate Status Protocol (OCSP) on the BIG-IP system.

1. Import root CA certificate to the BIG-IP

2. In the GUI go to **System > Certificate Management: Traffic Certificate Management: OCSP** and create an OCSP responder configuration
3. In **SSL Configurations**, deploy SSLO L3 Outbound topology
    a. Reference the OCSP server under **OCSP Certificate Validator**
    b. Reference the imported CA certificate under **Trusted Certificate Authority**

The following article, ***K75106155: Configuring OCSP stapling (13.x – 16.x)***, has additional information for OCSP configuration and OCSP stapling on the BIG-IP.

4 Appendix: ccmode command

The ccmode command is a command script used during the configuration of a Common-Criteria-evaluation-compliant system to easily make a subset of the required configuration changes.

While running this command is essential to creating a Common-Criteria-compliant system, it is not intended to be the only step. The instructions in this Common Criteria Guidance Supplement document must be followed to completely configure a compliant BIG-IP.

This command has no facility for "undoing" the changes it makes. Instead, the administrator must reverse or revise all of the individual commands, reset the DB variables to their defaults, save the new configuration, and restart the BIG-IP.

The following commands are issued from ccmode command script.

Command	Description
tmsh modify net self-allow defaults none	Set up the self-ip ports to allow=none.
tmsh modify /sys daemon-log-settings mcpd audit enabled **tmsh modify /sys daemon-log-settings tmm os-log-level error**	Enable mcpd and tmm logging and set the proper log levels. This ensures that each GUI and tmsh command are properly audited.
tmsh modify /sys db log.ssl.level value informational	Ensure that the TLS logging is set for proper auditing.
tmsh modify /sys global-settings lcd-display disabled	Disable the front panel LCD display and input.
tmsh modify /sys service snmpd disable	Disable snmpd.
… use an internal (to ccmode) routine to generate a new device key …	Ensure that a new device key, using only restricted ciphers, is generated.
tmsh modify /sys httpd (ssl-ciphersuite EECDH+AES:RSA+AES:@STRENGTH ssl-protocol all -SSLv2 -SSLv3 -TLSv1)	Ensure that httpd uses only supported TLS ciphersuites and versions.
tmsh modify /ltm profile client-ssl clientssl ciphers cc_stip **tmsh modify /ltm profile server-ssl serverssl ciphers cc_stip**	Ensure that SSL profiles only use the restricted set of ciphers.
tmsh modify /sys db security.commoncriteria.stip value true	Tell the system to invoke STIP Common Criteria-specific runtime code.
tmsh modify /sys db ssl.forwardproxy.inspectionconsent value yes	Intercept SSL/TLS encrypted traffic:
tmsh modify /auth password-policy policy-enforcement enabled minimum-length 15 required-uppercase 1 required-lowercase 1 required-numeric 1 required-special 1 max-duration 90 expiration-warning 7 max-login-failures 3 password-memory 3	Set the default password policy: • Minimum length of password = 15 • At least 1 uppercase character • At least 1 lowercase character • At least 1 numeric character • At least 1 special character • Password expires in 90 days

	• The user gets a warning 7 days before the expiration • The user can attempt to login unsuccessfully 3 times before being locked out • The password cannot be repeated within the last 3 passwords.
tmsh modify cli global-settings idle-timeout 20 **tmsh modify /sys httpd auth-pam-idle-timeout 1200** **tmsh modify /sys sshd inactivity-timeout 1200** **tmsh modify /sys global-settings console-inactivity-timeout 1200**	Set the autologout time for a tmsh session, GUI session, and SSH session to 20 minutes.
tmsh run util sys-icheck	Run the sys-icheck utility to validate the RPM files. sys-icheck is a thin wrapper around RPM package validation; it uses a stored checksum for every filesystem object and validates that checksum for every installed package (code, static data, and system configuration). The one change from RPM validation is that sys-icheck will issue a warning if a modified configuration file has an unmodified backup, but an error if it does not.
tmsh modify /sys db liveinstall.checksig value enable	Ensure that all install files applied after initial configuration must pass software archive signature validation. (Note that signature validation is a required step in the installation of the Common Criteria-evaluated system, which covers the initial install case.)
tmsh modify /sys db provision.action value reboot	Update the prompt to remind the administrative-user to reboot once the ccmode command has completed.
tmsh modify /sys db security.commoncriteria value true	Tell the system to invoke Common Criteria-specific runtime code.
tmsh modify /sys db statemirror.secure value enable **tmsh modify /sys db failover.secure value enable**	Ensure that the failover communications channels are secure (encrypted)
tmsh modify /sys db systemauth.disablelocaladminlockout value true **tmsh modify /sys db systemauth.disablemanualunlock value true** **tmsh modify /sys db password.unlock_time value 600**	Ensure that the primary administrative user may login locally even if locked out remotely. Disable the manual lockout commands and use the time unlock instead. Set the unlock_time value to 600 seconds (10 minutes).
/usr/bin/bigstart add fault_monitord	Enable the daemon that tracks certain failures
tmsh -q modify /sys aom readonly enabled **tmsh modify /sys aom media-redirection disabled** **tmsh modify /sys aom vkvm disabled** **tmsh modify /sys aom webui disabled** **tmsh modify /sys aom ipmi disabled**	AOM specific commands

tmsh save /sys configbigstart add fault_monitord	Enable fault_monitord daemonSave the configuration
tmsh save /sys config	Save the configuration

Table 4: ccmode command

5 Appendix: Allowed Ciphersuites for TLS and SSH

5.1 TLS

The following table summarizes the cipher suites supported by the evaluated configuration for TLS connections. All other proposed cipher suites are rejected.

Cipher	Data Plane Client	Data Plane Server	Control Plane Server
TLS_RSA_WITH_AES_128_CBC_SHA	TLS v1.1, v1.2	TLS v1.1, v1.2	N/A
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLS v1.1, v1.2	TLS v1.1, v1.2	TLS v1.1, v1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLS v1.1, v1.2	TLS v1.1, v1.2	TLS v1.1, v1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLS v1.1, v1.2	TLS v1.1, v1.2	N/A
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLS v1.1, v1.2	TLS v1.1, v1.2	N/A
TLS_RSA_WITH_AES_128_CBC_SHA256	TLS v1.2	TLS v1.2	TLS v1.2
TLS_RSA_WITH_AES_256_CBC_SHA256	TLS v1.2	TLS v1.2	TLS v1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLS v1.2	TLS v1.2	N/A
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLS v1.2	TLS v1.2	N/A
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLS v1.2	TLS v1.2	N/A
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLS v1.2	TLS v1.2	N/A
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLS v1.2	TLS v1.2	TLS v1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLS v1.2	TLS v1.2	TLS v1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLS v1.2	TLS v1.2	TLS v1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLS v1.2	TLS v1.2	TLS v1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	N/A	N/A	TLS v1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	N/A	N/A	TLS v1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_256_CCM	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_RSA_WITH_AES_256_CCM	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_128_CCM	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_RSA_WITH_AES_128_CCM	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_RSA_WITH_AES_256_CBC_SHA	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_RSA_WITH_AES_128_CCM_8	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_128_CCM_8	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_DHE_RSA_WITH_AES_256_CCM_8	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A
TLS_RSA_WITH_AES_256_CCM_8	TLS v1.0, 1.1, 1.2	TLS v1.0, 1.1, 1.2	N/A

Table 5: Allowed ciphersuites for TLS

5.2 SSH Server Protocol

- Encryption Algorithms
  - AES128-CBC
  - AES256-CBC
  - AES128-CTR
  - AES256-CTR
- Public-key algorithms
  - ecdsa-sha2-nistp256
  - ecdsa-sha2-nistp384
- MAC algorithms
  - hmac-sha1
  - hmac-sha2-256
- Key exchange methods
  - ecdsa-sha2-nistp256
  - ecdsa-sha2-nistp384

6 Appendix: Corrections to Published Documentation

6.1 BIG-IP Systems: Getting Started Guide

The **BIG-IP Systems: Getting Started Guide** was last updated for BIG-IP version 10.1 but is still valid for current releases, with the following exceptions:

- References to installation and upgrade from versions 9.3.x and 9.4.x to 10.1.x including sections in Chapter 2, Chapter 3, and Appendix A.
- Some commands or GUI references may have changed; see the current ***tmsh Reference Guide*** and GUI online help for the definitive definitions.

7 Appendix: Disallowed tmsh Commands

The following tmsh commands are not included or not allowed in the evaluated configuration.

global publish
analytics application-security commands
analytics protocol-security report
analytics sip-dos report
auth radius
auth radius-server
auth tacacs
gtm commands
gtm global-settings commands
gtm monitor commands
ltm auth crldp-server
lmt auth kerberos-delegation
ltm auth ocsp-responder
ltm-auth radius
ltm auth radius-server
ltm auth ssl-crldp
ltm auth tacacs
ltm classification commands
ltm monitor diameter
ltm monitor radius
ltm monitor radius-accounting
ltm monitor sip
ltm persistence dest-addr
ltm persistence global-settings
ltm persistence hash
ltm persistence msrdp
ltm persistence persist-records
ltm persistence sip
ltm persistence ssl
ltm persistence universal
ltm profile analytics
ltm profile diameter
ltm profile ntlm
ltm profile radius
ltm profile rtsp
ltm profile sctp
ltm profile sip
ltm profile stream
ltm profile web-acceleration
ltm profile web-security
net fdb commands
net ipsec commands
pem commands
pem profile commands
pem reporting commands
sys geoip
sys smtp-server
sys snmp
sys application commands
sys crypto crl
sys file ssl-crl
sys log-config dest arcsight
sys log-config dest local-database
sys log-config splunk
sys sflow commands
sys sflow data-source commands
sys sflow global-settings commands
util commands
wam commnds
wam global-settings commands
wam resource commands
wom commands
wom profile commands

apm commands

asm commands

8 Appendix: Disallowed iControl APIs

The following iControl modules are not included or not allowed in the evaluated configuration:

ARX
ASM
PEM
WebAccelerator

The following iControl module interfaces are not included or not allowed in the evaluated configuration:

GlobalLB Application
GlobalLB PoolMember
GlobalLB VirtualServer
LocalLB NAT
LocalLBNodeAddress
LocalLB ProfileDiameter
LocalLB ProfileDiameterEndpoint
LocalLB ProfileRADIUS
LocalLB ProfileRTSP
LocalLB ProfileSCTP
LocalLB ProfileSIP
LocalLB ProfileStream
LocalLB VirtualAddress
Log DestinationArcSight
Log DestinationSplunk
Management CRLDPConfiguration
Management CRLDPServer
Management OCSPConfiguration
Management OCSPResponder
Management RADIUSConfiguration
Management RADIUSServer
Management SMTPConfiguration
Management SNMPConfiguration
Management TACACSConfiguration
Networking IPsecIkeDaemon
Networking IPsecIkePeer
Networking
IPsecManualSecurityAssociation
Networking IPsecPolicy
Networking IPsecTrafficSelector
Networking RouteDomain
Networking RouteTable
Networking STPInstance
Networking SelfIP
Networking SelfIPPortLockdown
Networking Tunnel
Networking VLAN
Networking VLANGroup
Networking iSessionAdvertisedRoute
Networking iSessionRemoteInterface
System GeoIP
System PerformanceSFlow

9 Appendix: Audit and Event Records

9.1 Event Record Formats

9.1.1 Event Record Information Categories

The following table describes the information included in each event record, based on the log to which it is written.

Event Content		Log Type				
		System	Packet Filter	Local traffic	Audit (mcp)	Audit (other)
Timestamp	The time and date that the system logged the event message.	X	X	X	X	X
Log Level	Provides log level detail for each message.					
Host name	The host name of the system that logged the event message.	X	X	X		X
Service	The service that generated the event.	X	X	X		X
Status Code	The status code associated with the event.		X		X	
Session ID	The ID associated with the user session.					
Description	The description of the event that caused the system to log the message.	X	X	X	X	X
User name	The name of the user who made the configuration change.				X	X
Transaction ID	The identification number of the configuration change.				X	
Event	A description of the configuration change that caused the system to log the message.				X	

Table 6: Event record content

9.2 Sample Event Records – TMOS

This section contains samples of event records generated by TMOS.

Note: timestamped entries in the sections below are the actual event records. Items in ***bold italic*** are explanations of the record.

9.2.1 Start-up of audit functions

The following log entry is a sample from system startup, and indicates that auditing is active.

```
Jul 30 12:35:45 BIGIP138 notice 10syslog.sysinit: syslog-ng startup succeeded
```

The following log entry is a sample created when logging is re-enabled after being disabled while the BIG-IP is running.

```
Jul 29 15:56:22 BIGIP138 notice mcpd[6112]: 01070417:5: AUDIT - user admin - transaction #2372153-3 - object
0 - create_if { ltcfg_instance_field { ltcfg_instance_field_instance_name "/Common/cli"
ltcfg_instance_field_field_name "audit" ltcfg_instance_field_class_name "cli" ltcfg_instance_field_container ""
ltcfg_instance_field_value "enable" ltcfg_instance_field_userspec 1 ltcfg_instance_field_config_source 0 } }
[Status=Command OK]
```

9.2.2 Shutdown of audit functions

```
May 11 15:33:58 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmsh, tmsh-pid-15486, user root -
transaction #5126916-2 - object 0 - modify { db_variable { db_variable_name "config.auditing"
db_variable_value "disable" } } [Status=Command OK]
May 11 15:33:58 b6-2 notice tmsh[15486]: 01420002:5: AUDIT - pid=15486 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=modify /sys db config.auditing value disable
```

9.2.3 Administrative actions

9.2.3.1 Administrator Login

```
May 11 16:01:19 b6-2 notice httpd[4711]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam):
user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin host=192.168.43.159 attempts=1
start="Thu May 11 16:01:19 2017".
```

9.2.3.2 Administrator Logout

```
May 11 16:01:55 b6-2 notice httpd[19512]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam):
user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin host=192.168.43.159 attempts=1
start="Thu May 11 16:01:19 2017" end="Thu May 11 16:01:55 2017".
```

9.2.3.3 System Configuration Changes

This section includes samples of general security-related configuration changes for each user interface, and for mcpd (the internal configuration processor).

9.2.3.3.1 mcpd-level logs

All system configuration changes (MCP audit-logging must be turned on) are of the following format. In this case, the command was to modify the DB variable "Config.Auditing" to value "verbose".

```
	Jul  9 04:26:14 foo notice mcpd[7659]: 01070417:5: AUDIT - user admin - transaction #326837-2 - object 0 -
modify { db_variable { db_variable_name "config.auditing" db_variable_value "verbose" } } [Status=Command
OK]
```

9.2.3.3.2 tmsh

TMSH command line auditing in /var/log/audit (tmsh audit-logging must be turned on). The first event is the success case for command "list sys db"; the second is the failure case for the command "show db".

```
 Jul  9 04:01:02 foo notice tmsh[10416]: 01420002:5: AUDIT - pid=10416 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=list sys db

Sep  9 17:25:41 BIGIP138 notice -tmsh[808]: 01420002:5: AUDIT - pid=808 user=admin folder=/Common
module=(tmos)# status=[Syntax Error: "DB" unexpected argument] cmd_data=show DB
```

9.2.3.3.3 GUI

The GUI relies on mcpd to handle its logging. The following is the result of the GUI panel request to modify the DB variable "log.mcpd.level" to value "warning".

```
Apr 20 22:15:05 b6-1 notice mcpd[9625]: 01070417:5: AUDIT - client tmui, user admin - transaction #199368-2 - object 0 - modify { db_variable { db_variable_name "log.mcpd.level" db_variable_value "warning" } } [Status=Command OK]iControl (SOAP)
```

9.2.3.3.4 iControl

iControl and mcpd both log iControl administrative functions. In this case, iControl is creating a new pool called "mw_pool".

```
Jul 30 11:40:30 sip-repro debug iControlPortal.cgi[22592]: LocalLB:+++++++++++++++new+++++++++++++++++++
Jul 30 11:40:30 sip-repro debug iControlPortal.cgi[22592]: LocalLB:Pool::create called by user "admin"
Jul 30 11:40:30 sip-repro debug iControlPortal.cgi[22592]: LocalLB:   [0] Name: mw_pool
Jul 30 11:40:30 sip-repro debug iControlPortal.cgi[22592]: LocalLB:       Load Balancing Method: 0
Jul 30 11:40:30 sip-repro debug iControlPortal.cgi[22592]: LocalLB:   [0] (note: empty children)Pool: mw_pool
Jul 30 11:40:30 sip-repro debug iControlPortal.cgi[22592]: LocalLB:+++++++++++++++new+++++++++++++++++++

Jul 30 11:40:30 Received request message from connection 0x5d2edcc8 (user admin):
start_transaction {
}

Jul 30 11:40:30 Received request message from connection 0x5d2edcc8 (user admin):
mcpd_context {
  mcpd_context_folder "/Common"
  mcpd_context_recursive_query 0
  mcpd_context_normalize_ip_address_rd 1
}
create {
  pool {
    pool_name "mw_pool"
    pool_lb_mode 0
  }
}

Jul 30 11:40:30 Received request message from connection 0x5d2edcc8 (user admin):
end_transaction {
}
```

9.2.3.3.5 iControl REST

The first example below is the success event record for the iControl REST command to create a virtual server; the second is a failure to create a virtual server attached to a non-existent pool.

```
May 11 16:13:09 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmsh, tmsh-pid-28602, user admin - transaction #5156785-2 - object 0 - create { virtual_server { virtual_server_name "/Common/vs" virtual_server_va_name "10.10.10.100" virtual_server_port http virtual_server_default_pool "non_existent_pool" } } [Status=Command OK]
May 11 16:13:09 b6-2 notice icrd_child[28602]: 01420002:5: AUDIT - pid=28602 user=admin folder=/Common
module=(tmos)# status=[01020036:3: The requested pool (non_existent_pool) was not found.]
cmd_data=create ltm virtual /Common/vs { destination 10.10.10.100:80 pool non_existent_pool }
```

9.2.3.4 Cryptographic Key Administrative Actions

9.2.3.4.1 Generating a Key

```
May 11 16:20:14 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client iControlSOAP, user admin - transaction
#5165256-2 - object 0 - create { certificate_key_file_object { certificate_key_file_object_name
"/Common/Generating-a-Key.key" certificate_key_file_object_checksum
"SHA1:1704:8e351d641eb5925fc3a58f3dae02d48424efaa83" certificate_key_file_object_local_path
"/config/ssl/ssl.key/Generating-a-Key.key" certificate_key_file_object_source_path
"/config/ssl/ssl.key/Generating-a-Key.key" certificate_key_file_object_security_type 0 } } [Status=Command OK]
May 11 16:20:14 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client iControlSOAP, user admin - transaction
#5165264-2 - object 0 - create_if { certificate_file_object { certificate_file_object_name "/Common/Generating-
a-Key.crt" certificate_file_object_checksum "SHA1:1249:52d2291766cb12ae0e74ed5544562baa0f46eeec"
certificate_file_object_local_path "/config/ssl/ssl.crt/Generating-a-Key.crt" certificate_file_object_source_path
"/config/ssl/ssl.crt/Generating-a-Key.crt" } } [Status=Command OK]
May 11 16:20:14 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5165270-2
- object 0 - modify { db_variable { db_variable_name "ssl.certrequest.commonname" db_variable_value "123" } }
[Status=Command OK]
May 11 16:20:14 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5165274-2
- object 0 - modify { db_variable { db_variable_name "ssl.certrequest.divisionname" db_variable_value "1" } }
[Status=Command OK]
May 11 16:20:14 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5165278-2
- object 0 - modify { db_variable { db_variable_name "ssl.certrequest.organizationname" db_variable_value
"abc" } } [Status=Command OK]
May 11 16:20:14 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5165282-2
- object 0 - modify { db_variable { db_variable_name "ssl.certrequest.localityname" db_variable_value "b" } }
[Status=Command OK]
May 11 16:20:14 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5165289-2
- object 0 - modify { db_variable { db_variable_name "ssl.certrequest.stateorprovincename" db_variable_value
"WA" } } [Status=Command OK]
May 11 16:20:14 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5165293-2
- object 0 - modify { db_variable { db_variable_name "ssl.certrequest.countryname" db_variable_value "US" } }
[Status=Command OK]
May 11 16:20:15 b6-2 notice tmsh[21987]: 01420002:5: AUDIT - pid=21987 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=save / sys config partitions all
```

9.2.3.4.2 Importing a Key

```
May 11 16:29:41 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5199445-2
- object 0 - create { certificate_key_file_object { certificate_key_file_object_name "/Common/Importing-a-
Key.key" certificate_key_file_object_checksum "SHA1:1704:eff681ec11870035d3d31f1fa1f0afbf1799b51e"
certificate_key_file_object_local_path "/tmp/Importing-a-Key.key" certificate_key_file_object_security_type 0 }
} [Status=Command OK]
```

```
May 11 16:29:42 b6-2 notice tmsh[23333]: 01420002:5: AUDIT - pid=23333 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=save / sys config partitions all
```

9.2.3.4.3 Changing a Key

```
May 11 16:27:36 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5183414-2
- object 0 - modify { certificate_key_file_object { certificate_key_file_object_name "/Common/Generating-a-
Key.key" certificate_key_file_object_checksum "SHA1:2484:f21d73cb2f1d6ddc5bf9ace871b23fc617848308"
certificate_key_file_object_local_path "/tmp/Generating-a-Key.key" certificate_key_file_object_security_type 0
} } [Status=Command OK]
May 11 16:27:37 b6-2 notice tmsh[23009]: 01420002:5: AUDIT - pid=23009 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=save / sys config partitions all
```

9.2.3.4.4 Deleting a Key

```
May 11 16:28:09 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5188244-2
- object 0 - obj_delete { certificate_key_file_object { certificate_key_file_object_name "/Common/Generating-a-
Key.key" } } [Status=Command OK]
May 11 16:28:10 b6-2 notice tmsh[23099]: 01420002:5: AUDIT - pid=23099 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=save / sys config partitions all
```

9.2.3.5 Resetting Passwords

```
May 11 16:36:37 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5250742-3
- object 0 - modify { db_variable { db_variable_name "systemauth.disablerootlogin" db_variable_value "false" } }
[Status=Command OK]
May 11 16:36:37 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5250742-4
- object 0 - modify { db_variable { db_variable_name "service.ssh" db_variable_value "enable" } }
[Status=Command OK]
May 11 16:36:37 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5250742-5
- object 0 - modify { ltcfg_instance { ltcfg_instance_name "/Common/system" ltcfg_instance_class_name
"system" ltcfg_instance_instance_folder_name "/Common" ltcfg_instance_instance_leaf_name "system"
ltcfg_instance_config_source 0 } } [Status=Command OK]
May 11 16:36:37 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5250742-7
- object 0 - modify { folder { folder_name "/" folder_traffic_group "/Common/traffic-group-1" } }
[Status=Command OK]
May 11 16:36:37 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5250742-6
- object 0 - modify { ltcfg_instance_field { ltcfg_instance_field_instance_name "/Common/system"
ltcfg_instance_field_field_name "mgmt_dhcp" ltcfg_instance_field_class_name "system"
ltcfg_instance_field_container "" ltcfg_instance_field_object_id 14039 ltcfg_instance_field_value "false"
ltcfg_instance_field_userspec 1 ltcfg_instance_field_config_source 0 } } [Status=Command OK]
tem" ltcfg_instance_instance_folder_name "/Common" ltcfg_instance_instance_leaf_name "system"
ltcfg_instance_config_source 0 } } [Status=Command OK]
May 11 16:36:37 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5250742-7
- object 0 - modify { folder { folder_name "/" folder_traffic_group "/Common/traffic-group-1" } }
[Status=Command OK]
```

```
May 11 16:36:37 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5250742-6
- object 0 - modify { ltcfg_instance_field { ltcfg_instance_field_instance_name "/Common/system"
ltcfg_instance_field_field_name "mgmt_dhcp" ltcfg_instance_field_class_name "system"
ltcfg_instance_field_container "" ltcfg_instance_field_object_id 14039 ltcfg_instance_field_value "false"
ltcfg_instance_field_userspec 1 ltcfg_instance_field_config_source 0 } } [Status=Command OK]
May 11 16:36:37 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #5250774-2
- object 0 - modify { userdb_entry { userdb_entry_name "root" userdb_entry_passwd "***"
userdb_entry_is_crypted 0 } } [Status=Command OK]
May 11 16:36:38 b6-2 notice tmsh[24581]: 01420002:5: AUDIT - pid=24581 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=save / sys config partitions all
```

9.2.3.6 Starting Services

```
May 11 16:40:12 b6-2 notice tmsh[25327]: 01420002:5: AUDIT - pid=25327 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=start /sys service big3d
```

9.2.3.7 Stopping Services

```
May 11 16:39:49 b6-2 notice tmsh[25327]: 01420002:5: AUDIT - pid=25327 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=stop /sys service big3d
```

9.2.4 Warning for Low Local Audit Storage Space (FAU_STG_EXT.3/LocSpace)

```
[root@b6-2:sflow_agent DOWN:In Sync] log # May 12 16:50:23 b6-2 emerg alertd[8825]: 01100048:0: Log disk
usage still higher than 80% after logrotate and 24 times log deletion
Broadcast message from root@b6-2.platsec.pdsea.f5net.com (Fri May 12 16:51:02 2017):
011d0004:3: Disk partition /var/log has only 0% free
```

9.2.5 Failure to Establish an HTTPS Session (FCS_HTTPS_EXT.1)

In the following examples, the first two session requests failed because the admin user has "nologin" specified in the BIG-IP configuration, and so login is denied. In the third case, the error message is returned from mod_auth_pam(), which means that the login authentication failed.

From /var/log/audit:

```
    Apr 21 18:13:09 b6-1 notice httpd[23439]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam):
user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin host=192.168.43.146 attempts=1
start="Fri Apr 21 18:13:09 2017".
    Apr 21 18:12:39 b6-1 notice httpd[24589]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam):
user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin host=192.168.43.146 attempts=1
start="Fri Apr 21 17:53:27 2017" end="Fri Apr 21 18:12:39 2017".
    Apr 20 22:18:11 b6-1 info httpd(pam_audit)[13209]: 01070417:6: AUDIT - user 1234 - RAW:
httpd(pam_audit): User=1234 tty=(unknown) host=172.18.43.28 failed to login after 1 attempts (start="Thu Apr
20 22:18:09 2017" end="Thu Apr 20 22:18:11 2017").
```

From /var/log/ltm (log.ssl.level set to Informational):

```
   Jun 27 14:41:18 sjctmos-3600-224 info tmm1[16155]: 01260013:6: SSL Handshake failed for TCP from
10.100.36.54:57278 to 10.100.36.99:443
```

```
    Jun 27 14:41:31 sjctmos-3600-224 info tmm1[16155]: 01260019:6: SSL Handshake succeeded for TCP from
10.100.36.54:57294 to 10.100.36.99:443
    Jun 27 14:41:33 sjctmos-3600-224 info tmm1[16155]: 01260020:6: SSL Connection terminated for TCP from
10.100.36.54:57294 to 10.100.36.99:443
```

9.2.6 Failure to Establish an SSH Session (BIG-IP as Server) (FCS_SSHS_EXT.1)

In the event records below, the entries are coming from pam_audit(). In the first two, the SSH session is not established because user root is not allowed to log in when Appliance Mode is licensed (as it must be for the Common Criteria configuration. In the third case, the user "asdf" doesn't exist.

From /var/log/audit:

```
    Jul  9 03:26:07 foo info sshd(pam_audit)[10153]: 01070417:6: AUDIT - user root - RAW: sshd(pam_audit):
user=root(root) partition=[All] level=Administrator tty=ssh host=172.27.226.130 attempts=1 start="Tue Jul  9
03:26:07 2013".
    Jul  9 03:26:10 foo info sshd(pam_audit)[10153]: 01070417:6: AUDIT - user root - RAW: sshd(pam_audit):
user=root(root) partition=[All] level=Administrator tty=ssh host=172.27.226.130 attempts=1 start="Tue Jul  9
03:26:07 2013" end="Tue Jul  9 03:26:10 2013".
    Jul  9 03:26:35 foo info sshd(pam_audit)[10191]: 01070417:6: AUDIT - user asdf - RAW: sshd(pam_audit):
User=asdf tty=ssh host=172.27.226.130 failed to login after 1 attempts (start="Tue Jul  9 03:26:31 2013"
end="Tue Jul  9 03:26:35 2013").
```

9.2.7 Failure to Establish a TLS Data Plane Session (BIG-IP as Client) (FCS_TLSC_EXT.2)

From /var/log/ltm:

```
Aug  8 14:37:06 b6-2 info tmm[10834]: 01260019:6: SSL Handshake succeeded for TCP 10.60.189.128:43252 ->
10.60.206.206:443
Aug  8 14:37:06 b6-2 warning tmm[10834]: 01260006:4: Peer cert verify error: self signed certificate in
certificate chain (depth 2; cert /C=US/ST=Washington/L=Seattle/O=F5 Networks, Inc./OU=F5 Test/CN=F5 CC
Test Root CA)
Aug  8 14:37:06 b6-2 warning tmm[10834]: 01260009:4: Connection error: ssl_shim_vfycerterr:4539: self signed
certificate in certificate chain (48)
Aug  8 14:37:06 b6-2 info tmm[10834]: 01260020:6: SSL Connection terminated for TCP 10.60.189.128:43252 ->
10.60.206.206:443
Aug  8 14:37:06 b6-2 info tmm[10834]: 01260020:6: SSL Connection terminated for TCP 10.60.189.128:43252 ->
10.60.206.206:443
Aug  8 14:37:06 b6-2 info tmm[10834]: 01260013:6: SSL Handshake failed for TCP 10.7.186.187:443 ->
10.7.204.254:43252
```

9.2.8 Failure to Establish a TLS Data Plane Session (BIG-IP as Server) (FCS_TLSS_EXT.1)

From /var/log/ltm, the following error says that the protocol version is unsupported (note that the error code is from the SSL RFC 5246):

```
May 18 15:57:55 b6-2 warning tmm3[13093]: 01260009:4: Connection error: ssl_hs_rxhello:7429: unsupported version (70)
May 18 15:57:55 b6-2 info tmm3[13093]: 01260013:6: SSL Handshake failed for TCP 10.60.171.1:51044 -> 10.60.204.24:443
```

9.2.9 FIA_AFL.1

Same as FIA_UAU_EXT.2 for log entries.

9.2.10 Identification and Authentication (FIA_UIA_EXT.1)

Same as FIA_UAU_EXT.2 for log entries.

9.2.11 Password-based Authentication (FIA_UAU_EXT.2)

From /var/log/audit:

Login via GUI:

```
Apr 21 18:16:35 b6-1 notice httpd[24588]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam): user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin host=192.168.43.146 attempts=1 start="Fri Apr 21 18:16:35 2017".
```

Login via SSH:

```
Apr 21 18:18:04 b6-1 info sshd(pam_audit)[24218]: 01070417:6: AUDIT - user root - RAW: sshd(pam_audit): user=root(root) partition=[All] level=Administrator tty=ssh host=172.27.17.161 attempts=1 start="Fri Apr 21 18:18:04 2017".
```

Login via iControl:

```
Nov 29 14:47:35 b3-2 notice httpd[11589]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam): user=admin(admin) partition=[All] level=Administrator tty=/usr/bin/tmsh host=192.168.43.164 attempts=1 start="Wed Nov 29 14:47:35 2017".
```

Login via iControl REST:

```
Nov  7 14:26:08 b3-2 notice httpd[17220]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam): user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin host=172.27.17.188 attempts=1 start="Tue Nov  7 13:55:42 2017" end="Tue Nov  7 14:26:08 2017".
```

Failed login via GUI:

```
Apr 21 18:19:50 b6-1 info httpd(pam_audit)[24588]: 01070417:6: AUDIT - user admin - RAW: httpd(pam_audit): User=admin tty=(unknown) host=192.168.43.146 failed to login after 1 attempts (start="Fri Apr 21 18:19:47 2017" end="Fri Apr 21 18:19:50 2017").
```

Failed login via SSH:

```
Sep  9 17:05:27 BIGIP138 info sshd(pam_audit)[32342]: 01070417:6: AUDIT - user admin - RAW: sshd(pam_audit): User=admin tty=ssh host=172.17.2.54 failed to login after 1 attempts (start="Tue Sep  9 17:04:54 2014" end="Tue Sep  9 17:05:27 2014").
```

Failed login via iControl:

```
Sep 12 13:39:23 localhost info httpd(pam_audit)[9983]: 01070417:6: AUDIT - user admin - RAW: httpd(pam_audit): User=admin tty=(unknown) host=192.168.24.3 failed to login after 1 attempts (start="Tue Sep 12 13:39:21 2017" end="Tue Sep 12 13:39:23 2017").
```

Failed login via iControl REST:

```
Sep 12 13:42:04 localhost info httpd(pam_audit)[27004]: 01070417:6: AUDIT - user admin - RAW:
httpd(pam_audit): User=admin tty=(unknown) host=192.168.24.3 failed to login after 1 attempts (start="Tue
Sep 12 13:42:01 2017" end="Tue Sep 12 13:42:04 2017").
```

9.2.12 Certificate Validation (FIA_X509_EXT.1/REV)

From /var/log/audit:

```
May 12 17:47:43 b6-2 notice mcpd[8291]: 01070417:5: AUDIT - client tmui, user admin - transaction #6166138-2
- object 0 - modify { certificate_file_object { certificate_file_object_name "/Common/temp-x509-cert-
validation.crt" certificate_file_object_checksum "SHA1:1919:d0f30074e9185524b00eafda8d50863cfd44226c"
certificate_file_object_local_path "/tmp/temp-x509-cert-validation.crt" } } [Status=Command OK]
```

From /var/log/ltm:

```
May 12 17:47:43 b6-2 err mcpd[8291]: 01070712:3: Caught configuration exception (0), unable to validate
certificate, invalid x509 file (/Common/temp-x509-cert-validation.crt).
```

9.2.13 Restrict Management of Security Functions (FMT_MOF.1(1)/AdminAct)

The following log entries represent a GUI user setting up packet filtering on the BIG-IP; as a result of checkboxes in the GUI, several DB variables are set to accomplish this.

```
May 23 23:58:35 b6-2 notice mcpd[8293]: 01070417:5: AUDIT - client tmui, user admin - transaction #305659-2 -
object 0 - modify { db_variable { db_variable_name "packetfilter.sendicmperrors" db_variable_value "enable" } }
[Status=Command OK]
May 23 23:58:35 b6-2 notice mcpd[8293]: 01070417:5: AUDIT - client tmui, user admin - transaction #305663-2 -
object 0 - modify { db_variable { db_variable_name "packetfilter.established" db_variable_value "enable" } }
[Status=Command OK]
May 23 23:58:35 b6-2 notice mcpd[8293]: 01070417:5: AUDIT - client tmui, user admin -
transaction #305668-2 - object 0 - modify { db_variable { db_variable_name "packetfilter" db_variable_value
"enable" } } [Status=Command OK]
May 23 23:58:35 b6-2 notice mcpd[8293]: 01070417:5: AUDIT - client tmui, user admin - transaction #305673-2 -
object 0 - modify { packet_filter_allow_trusted { packet_filter_allow_trusted_address { }
packet_filter_allow_trusted_vlan { } packet_filter_allow_trusted_mac_addr { } } } [Status=Command OK]
```

9.2.14 Restrict Management of Services (FMT_MOF.1/Services)

The following event record stops and restarts the "big3d" daemon.

```
May 24 00:00:37 b6-2 notice logger: /usr/bin/syscalld  ==> /usr/bin/bigstart restart big3d
```

The following event records restart, stop, and start the http daemon:

```
Sep 12 13:45:45 localhost notice root: -bash  ==> /usr/bin/bigstart restart httpd
Sep 12 13:45:48 localhost notice root: -bash  ==> /usr/bin/bigstart stop httpd
Sep 12 13:45:50 localhost notice root: -bash  ==> /usr/bin/bigstart start httpd
```

9.2.15 Restrict Management of Updates (FMT_MOF.1/ManualUpdate)

The following is a record of a successful installation of BIG-IP 15.1.x on the volume "HD1.1".

```
May 24 12:28:14 b6-2 notice mcpd[8293]: 01070417:5: AUDIT - client tmui, user admin - transaction #783527-3 -
object 0 - modify { software_desired { software_desired_volume "HD1.1" software_desired_product "BIG-IP"
software_desired_version "16.1.3.1" software_desired_build "0.0.10" software_desired_active 0 } }
[Status=Command OK]
```

The following is a record (in /var/alog/audit) of a successful installation of BIG-IP 16.1.3.1 on the volume "HD1.2":

```
May 24 13:52:26 localhost notice mcpd[7111]: 01070417:5: AUDIT – client tmsh, tmsh-pid-29929, user root –
transaction #437059-2 – object 0 – modify { software_desired { software_desired_volume "HD1.2"
software_desired_product "BIG-IP" software_desired_version "16.1.3.1" software_desired_build "0.0.10"
software_desired_active 0 software_desired_retry 0 } } [Status=Command OK]
```

The following is a failure record (in/var/log/audit) for an update; the error is "Volume not found":

```
May 24 13:49:18 localhost notice tmsh[29798]: 01420002:5: AUDIT – pid=29798 user=root folder=/Common
module=(tmos)# status=[Data Input Error: volume not found "fake"] cmd_data=install sys software image BIGIP-
16.1.3.1-0.0.11.iso volume fake
```

9.2.16 Restrict Management of TSF Data (FMT_MTD.1/CoreData)

The following record creates a certificate file:

```
May 24 12:16:46 b6-2 notice mcpd[8293]: 01070417:5: AUDIT - client tmui, user admin - transaction #773066-2 -
object 0 - create { certificate_file_object { certificate_file_object_name "/Common/test-cert.crt"
certificate_file_object_checksum "SHA1:1913:4e80a1c128cbd8a47ae0145c5f4df2a70ce9052c"
certificate_file_object_local_path "/tmp/test-cert.crt" } } [Status=Command OK]
```

Execute "run util unix-rm -f /var/log/wccpd.log" by Guest user.
From /var/log/audit:

```
Nov  7 23:43:13 b3-2 notice -tmsh[7760]: 01420002:5: AUDIT - pid=7760 user=log-del folder=/Common
module=(tmos)# status=[Syntax Error: "unix-rm" unexpected argument] cmd_data=run util unix-rm
```

Resetting the administrative password from the command line using tmsh by Guest user.
From /var/log/audit:

```
Nov  8 15:55:27 b3-2 notice -tmsh[31609]: 01420002:5: AUDIT - pid=31609 user=log-del folder=/Common
module=(tmos)# status=[Syntax Error: "user" unexpected argument] cmd_data=modify auth user
```

9.2.17 Restrict Management of Cryptographic Keys (FMT_MTD.1/CryptoKeys)

```
May 24 00:20:52 b6-2 notice mcpd[8293]: 01070417:5: AUDIT - client tmui, user admin - transaction #337778-2 -
object 0 - obj_delete { certificate_key_file_object { certificate_key_file_object_name "/Common/md2-key.key" }
} [Status=Command OK]
```

9.2.18 Trusted Update (FPT_TUD_EXT.1)

See section *Error! Reference source not found.* **Error! Reference source not found.** ***for sample audit records for success or failure of the update. Note that all updates are full installs.***

9.2.19 Time Changes (FPT_STM_EXT.1.1)

The following records indicate a successful attempt to set the system clock using the tmsh "clock" command. The "audit" log contains the event records from the command execution of the tmsh modify clock command, including the time and date the command was executed (after the time change) as well as the time adjustment.

The "ltm" log contains the time change event record from the tmsh modify clock command, including the time and date the command was executed (before the time change) as well as the time adjustment.

To obtain the original time, adjustment, and final time, look at the following:

- ***Original time: timestamp on the tmsh modify clock command event record in the "ltm" log***
- ***Final time: timestamp on the tmsh modify clock command event record in the "audit" log***
- ***Time adjustment: tmsh modify clock command data from the event record in the "audit" log, and the event data from the event record in the "ltm" log.***

```
# tail audit
Sep 12 16:49:03 b10-1 notice tmsh[20079]: 01420002:5: AUDIT - pid=20079 user=root
folder=/Common module=(tmos)# status=[Command OK] cmd_data=modify sys clock time
now+2m
```

```
# tail ltm
Sep 12 16:47:06 b10-1 warning tmm1[16827]: 01010040:4: Clock has unexpectedly
adjusted by 119532 ms
```

9.2.20 Local Interactive Session Inactivity Timeout (FTA_SSL_EXT.1)

Timeout reached, user logged out:

```
 May 18 22:19:31 b6-1 notice tmsh[21434]: 01420002:5: AUDIT - User idle time out reached; logged out of tmsh.
```

Entry in /var/log/audit for command to unlock a locked-out user:

```
Nov  8 00:09:07 b3-2 notice tmsh[14844]: 01420002:5: AUDIT - pid=14844 user=root folder=/Common
module=(tmos)# status=[Command OK] cmd_data=reset-stats auth login-failures tmsh
```

9.2.21 Remote Interactive Session Inactivity Timeout (FTA_SSL.3)

```
      Jul  9 03:26:10 foo info sshd(pam_audit)[10153]: 01070417:6: AUDIT - user root - RAW: sshd(pam_audit):
user=root(root) partition=[All] level=Administrator tty=ssh host=172.27.226.130 attempts=1 start="Tue Jul  9
03:26:07 2013" end="Tue Jul  9 03:26:10 2013".
```

9.2.22 User Session Termination (FTA_SSL.4)

Timeout logs are the same as those listed above, eg:

```
     Jul  9 03:23:20 foo notice httpd[10093]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam):
user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin host=172.27.226.130 attempts=1
start="Tue Jul  9 03:23:14 2013" end="Tue Jul  9 03:23:20 2013".
```

9.2.23 Trusted Channel (FTP_ITC.1)

Syslog:

Encrypted syslog is effected by routing syslog through a TLS proxy;
encrypted syslog is not available on the management port

```
Nov 14 22:16:01 b3-2 info tmm4[16212]: 01260019:6: SSL Handshake succeeded for TCP 10.89.179.1:6514 ->
10.89.218.1:15968
Nov 14 22:17:01 b3-2 info tmm[16212]: 01260013:6: SSL Handshake failed for TCP 10.89.179.1:6514 ->
10.89.218.1:20787
Nov 14 22:26:06 b3-2 info tmm4[16212]: 01260020:6: SSL Connection terminated for TCP 10.89.179.1:6514 ->
10.89.218.1:15968
```

9.2.24 Trusted Path (FTP_TRP.1)

The following information is logged in /var/log/secure. It applies to GUI, iControl SOAP, and iControl REST paths.

Successful Login:

```
2018-04-12T15:01:51.072-07:00 chateau.pdsea.f5net.com notice httpd[25715]: 01070417:5: AUDIT - user admin
- RAW: httpd(mod_auth_pam): user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin
host=172.17.2.8 attempts=1 start="Thu Apr 12 15:01:51 2018".
```

Logout:

```
2018-04-12T15:03:49.520-07:00 chateau.pdsea.f5net.com notice httpd[25719]: 01070417:5: AUDIT - user admin
- RAW: httpd(mod_auth_pam): user=admin(admin) partition=[All] level=Administrator tty=/sbin/nologin
host=172.17.2.8 attempts=1 start="Thu Apr 12 15:01:51 2018" end="Thu Apr 12 15:03:49 2018".
```

Failed Login:

```
2018-04-12T15:05:24.719-07:00 chateau.pdsea.f5net.com info httpd(pam_audit)[9885]: User=admin
tty=(unknown) host=172.17.2.8 failed to login after 1 attempts (start="Thu Apr 12 15:05:22 2018" end="Thu Apr
12 15:05:24 2018").
```

The following information is logged in /var/log/audit when SSH connection is initiated:

```
        Nov 14 23:33:55 b3-2 info sshd(pam_audit)[29785]: 01070417:6: AUDIT - user root - RAW:
sshd(pam_audit): user=root(root) partition=[All] level=Administrator tty=ssh host=172.18.41.231 attempts=1
start="Tue Nov 14 23:33:55 2017".
```

The following information is logged in /var/log/ltm for SSH connections failures:

```
        Nov  8 08:35:46 b3-2 crit sshd[23227]: fatal: Unable to negotiate a key exchange method
```

The following information is logged in /var/log/secure when SSH connection is terminated:

```
        Nov 14 23:41:46 b3-2 info sshd(pam_audit)[31626]: user=root(root) partition=[All] level=Administrator
tty=ssh host=172.27.17.188 attempts=1 start="Tue Nov 14 23:41:06 2017" end="Tue Nov 14 23:41:46 2017".
Nov 14 23:41:46 b3-2 info sshd(pam_audit)[31626]: 01070417:6: AUDIT - user root - RAW: sshd(pam_audit):
user=root(root) partition=[All] level=Administrator tty=ssh host=172.27.17.188 attempts=1 start="Tue Nov 14
23:41:06 2017" end="Tue Nov 14 23:41:46 2017".
```

9.3 Sample Event Records – SSLO

This section contains samples of event records generated by SSLO.

Note: timestamped entries in the sections below are the actual event records. Items in ***bold italic*** are explanations of the record.

9.3.1 FCS_TTTC_EXT.1

Establishment of TLS session

```
        Nov 19 16:41:47 viomgmt01-17.auto.lab.fp.f5net.com info tmm1[12160]: 01260004:6:
/Common/ssloT_tls_settings.app/ssloT_tls_settings-sssl-vhf: SSL Handshake details for TCP 10.11.10.12:4433 ->
5.5.7.6:5 entity: client SID: e9b14509c02e34077581da154e13581aab6b8c99265efb4fbf14e50e11de2bce
version: TLSv1.2 client-cert-sha1: N/A server-cert-sha1:
96:6b:1c:a3:17:85:dc:0a:74:ed:86:1a:69:00:e0:8d:15:40:5f:d6 mutual-authentication: false
```

9.3.2 FCS_TTTS_EXT.1

Establishment of TLS session

See this AskF5 article for selecting cipher strength in SSL profiles (https://support.f5.com/csp/article/K01770517)

```
        Nov 19 16:41:47 viomgmt01-17.auto.lab.fp.f5net.com info tmm1[12160]: 01260004:6:
/Common/ssloT_tls_settings.app/ssloT_tls_settings-sssl-vhf: SSL Handshake details for TCP 10.11.10.12:4433 ->
5.5.7.6:5 entity: client SID: e9b14509c02e34077581da154e13581aab6b8c99265efb4fbf14e50e11de2bce
version: TLSv1.2 client-cert-sha1: N/A server-cert-sha1:
96:6b:1c:a3:17:85:dc:0a:74:ed:86:1a:69:00:e0:8d:15:40:5f:d6 mutual-authentication: false
```

9.3.3 FDP_CER_EXT.2

Linking of issued certificate to validated certificate

The following audit records in /var/log/ltm provide this linkage

```
        Feb  9 17:34:29 bigipve1mgmt.jvcforever.net info tmm[28298]: 01260019:6: SSL Handshake
succeeded for TCP 107.162.162.40:443 -> 192.168.0.210:50622
        Feb 9 17:34:29 bigipve1mgmt.jvcforever.net info tmm[28298]: 01260504:6:
/Common/ssloT_intercept.app/ssloT_intercept-sssl: SSL Handshake details for TCP 107.162.162.40:443 ->
192.168.0.210:50622 entity: client SID:
3403862ca9e71ab05d0a70be516f027993e06377aad9928499b65b66a07fd209 version: TLSv1.2 cipher-suite:
```

```
ECDHE-RSA-AES256-GCM-SHA384 key-exchange: 70 bytes client-cert-sha1: N/A server-cert-sha1:
e5:1d:f5:2b:2c:55:bb:44:d7:f4:78:bf:c2:8b:96:3c:66:10: f0:76 mutual-authentication: false
        Feb  9 17:34:29 bigipve1mgmt.jvcforever.net info tmm[28298]:
01260505:6: /Common/ssloT_intercept.app/ssloT_intercept-cssl: Private key of (null) is accessed to forge
certificate for SSL forward proxy CA for TCP 192.168.0.140:50622 -> 107.162.162.40:443 entity: server SID:
f4c346ec69a7db711dcaa035102fc239bbaba3b157cf1fcd59769ba6603f92c9
        Feb  9 17:34:29 bigipve1mgmt.jvcforever.net info tmm[28298]:
01260505:6: /Common/ssloT_intercept.app/ssloT_intercept-cssl: Private key of (null) is accessed to forge
certificate for SSL forward proxy CA for TCP 192.168.0.140:50622 -> 107.162.162.40:443 entity: server SID:
f4c346ec69a7db711dcaa035102fc239bbaba3b157cf1fcd59769ba6603f92c9
        Feb 9 17:34:29 bigipve1mgmt.jvcforever.net info tmm[28298]: 01260503:6:
/Common/ssloT_intercept.app/ssloT_intercept-cssl: SSL certificate forgery succeeded from server cert for TCP
192.168.0.140:50622 -> 107.162.162.40:443 entity: server SID:
f4c346ec69a7db711dcaa035102fc239bbaba3b157cf1fcd59769ba6603f92c9 original-cert-sha1:
e5:1d:f5:2b:2c:55:bb:44:d7:f4:78:bf:c2:8b:96:3c:66:10:f0:76 original-cert-dn:
/C=US/ST=Washington/L=Seattle/O=F5, Inc./CN=f5.com
        Feb  9 17:34:29 bigipve1mgmt.jvcforever.net info tmm[28298]: 01260019:6: SSL Handshake
succeeded for TCP 192.168.0.140:50622 -> 107.162.162.40:443
        Feb 9 17:34:29 bigipve1mgmt.jvcforever.net info tmm[28298]: 01260504:6:
/Common/ssloT_intercept.app/ssloT_intercept-cssl: SSL Handshake details for TCP 192.168.0.140:50622 ->
107.162.162.40:443 entity: server SID:
f4c346ec69a7db711dcaa035102fc239bbaba3b157cf1fcd59769ba6603f92c9 version: TLSv1.2 cipher-suite:
ECDHE-RSA-AES128-GCM-SHA256 key-exchange: 333 bytes client-cert-sha1: N/A server-cert-sha1:
e1:48:55:8f:a4:4e:fc:94:87:8d:6e :19:80:89:26:a4:99:91:f3:e6 mutual-authentication: false
```

9.3.4 FDP_CER_EXT.3

Issued Certificate generation

The audit record for the creation of the issued (forged) cert is found in /var/log/certificates.log

```
        Feb 9 17:34:29 bigipve1mgmt.jvcforever.net info tmm[28298]:
01d80000:6: /Common/ssloT_intercept.app/ssloT_intercept-cssl: Forged server certificate: SHA1:
e1:48:55:8f:a4:4e:fc:94:87:8d:6e:19:80:89:26:a4:99:91:f3:e6; SN: 7198334561636898224;
Subject: /C=US/ST=Washington/L=Seattle/O=F5, Inc./CN=f5.com; Certificate:
```

9.3.5 FDP_PPP_EXT.1

Configuration changes to the plaintext processing policy

```
        Fri, 19 Jun 2020 17:10:10 GMT - info: [SSLO] [Security Policy Create Success] Security policy
'/Common/ssloP_Test198' with rules:
[{"name":"Pinners_Rule","operation":"AND","mode":"edit","conditions":[{"index":1592586540202,"type":"SSL
Check","options":{"ssl":true,"url":[]}},{"index":1592586540203,"type":"SNI Category
Lookup","options":{"category":["Pinners"],"url":[]}}],"action":"allow","actionOptions":{"ssl":"bypass","serviceCh
ain":""},"index":1592586541394,"phase":2},{"name":"All
Traffic","action":"allow","mode":"edit","actionOptions":{"ssl":"intercept","serviceChain":""},"isDefault":true,"in
dex":1592586541395,"phase":2}]
```

```
        Fri, 19 Jun 2020 17:10:14 GMT - info: [SSLO] [Topology Create Success] Topology 'sslo_Test198'
```

9.3.6 FDP_PRC_EXT.1

Plaintext routed to inspection processing functional component

```
        Jun 9 13:02:54 amber-mgmt info tmm[2809]: 01c80043:6: CONNECTOR: Service at internal virtual
server
/Common/ssloS_GENERIC.app/ssloS_GENERIC-t-4 accepted internal connection; plaintext traffic on
(10.192.236.111:50976 -> 23.185.0.4:443) connection being routed to server (bytes len = 75).
```

9.3.7 FDP_STIP_EXT.1

Policy Action: Allow and intercept

```
        Mar 31 21:58:58 bigipssli info tmm[18760]: 01c40001:6:
/Common/sslo_l3_outbound.app/sslo_l3_outbound_accessProfile:Common:91ea241f:
/Common/sslo_l3_outbound.app/sslo_l3_outbound-in-t-4 Traffic summary - tcp 10.10.11.13:40974 ->
10.10.16.13:4433 clientSSL: TLSv1.2 ECDHE-RSA-AES128-GCM-SHA256 serverSSL: TLSv1.2 ECDHE-RSA-AES128-
GCM-SHA256 L7 https (f5.sslotest.com) decryption-status: decrypted duration: 48 msec service-path: ssloSC_sc1
client-bytes-in: 1154 client-bytes-out: 9229 server-bytes-in: 8090 server-bytes-out: 1075 policy-action: allow
client-side-SID: 7a90bceb4e54b04e62599ef3b69d58d71e30d4784cf4d8dc10885163862da8e7 server-side-SID:
daed497875900cb55307a9b0f3a9ab3b6f4beb0f9cd856355768259562479d56
```

Policy Action: Allow and bypass

```
        Oct 9 14:06:43 bigipssli info tmm[6293]: 01c40001:6:
/Common/sslo_test.app/sslo_test_accessProfile:Common:46a0cfc5: /Common/sslo_test.app/sslo_test-in-t-4
Traffic summary - tcp 10.10.11.13:48581 -> 93.184.216.34:443 clientSSL: NA NA serverSSL: NA NA L7 unknown
(example.com) decryption-status: not-decrypted duration: 130 msec service-path: NA client-bytes-in: 1259
client-bytes-out: 6960 server-bytes-in: 6756 server-bytes-out: 1335 policy-action: allow client-side-SID:
3e8421ff528954a2a6cd6a8f3a517cab38bfaa91b0b87e2d858398c80ae1ccbb server-side-SID: NA
```

Policy Action: Abort

```
        Oct 6 22:25:00 bigipssli info tmm[15605]: 01c40001:6:
/Common/sslo_test.app/sslo_test_accessProfile:Common:f02c6ec3: /Common/sslo_test.app/sslo_test-in-t-4
Traffic summary - tcp 10.10.11.13:48575 -> 93.184.216.34:443 clientSSL: TLSv1.2 ECDHE-RSA-AES128-GCM-
SHA256 serverSSL: NA NA L7 unknown (example.com) decryption-status: decrypted duration: 63 msec service-
path: NA client-bytes-in: 361 client-bytes-out: 167 server-bytes-in: 0 server-bytes-out: 0 policy-action: abort
client-side-SID: f90593d73c79776bc12d7c3b8520ff5230f8ab591d6e8fc56d23d65115700f22 server-side-SID: NA
```

Policy Action: Reject

```
        Oct 6 22:07:30 bigipssli info tmm[15605]: 01c40001:6:
/Common/sslo_test.app/sslo_test_accessProfile:Common:5ee7493e: /Common/sslo_test.app/sslo_test-in-t-4
Traffic summary - tcp 10.10.11.13:48573 -> 93.184.216.34:443 clientSSL: TLSv1.2 ECDHE-RSA-AES128-GCM-
SHA256 serverSSL: NA NA L7 https (example.com) decryption-status: decrypted duration: 93 msec service-path:
NA client-bytes-in: 1075 client-bytes-out: 4692 server-bytes-in: 0 server-bytes-out: 0 policy-action: block client-
side-SID: 82f80492d73c79776ac1249f3e8520ff88235c5c766bc078180a01f40e15700f server-side-SID: NA
```

9.3.8 FDP_TEP_EXT.1

Mutual authentication authorized

If Per-Request Policy log setting for the SSLO application is INFORMATION, a log message with the string “SSLO Session” will be printed in /var/log/apm after a client establishes a connection with SSLO

```
        Feb 27 20:01:55 bigipsslia.lab.fp.f5net.com notice tmm3[18378]: 01490505:5:
/Common/sslo_l3out.app/sslo_l3out_accessProfile:Common:582bf0d6: SSLO Session
```

When SSLO begins to evaluate the policy against the message, a log message with string “Starting per request access policy” will be printed in /var/log/apm

```
        Feb 27 20:01:55 bigipsslia.lab.fp.f5net.com info tmm3[18378]: 01870002:6:
/Common/sslo_l3out.app/sslo_l3out_accessProfile:Common:582bf0d6: Starting per request access policy
(/Common/ssloP_l3out.app/ssloP_l3out_pinners_rule_macro_policy)
```

Once the policy evaluation starts, policy handlers will be invoked at different protocol layers according to the policy configuration. If the policy execution determines that the client connection should be blocked, a log message indicating execution is done with ending type (Abort) will be printed in /var/log/apm

```
        Feb 27 20:01:55 bigipsslia.lab.fp.f5net.com info tmm3[18378]: 01870009:6:
/Common/sslo_l3out.app/sslo_l3out_accessProfile:Common:582bf
0d6: Execution of per request access policy (/Common/ssloP_l3out.app/ssloP_l3out_per_req_policy) done with
ending type (Abort)
```

If SSL Orchestrator Generic log setting for the application is INFORMATION, a log message will be printed in the /var/log/apm indicating that the client connection is aborted due to per-request policy decision

```
        Oct  8 16:11:46 bigipssli info tmm[6293]: 01c40002:6:
/Common/sslo_test.app/sslo_test_accessProfile:Common:842028bc: Traffic aborted for tcp 10.10.11.13:48579 -
> 93.184.216.34:443 (SID af42b9c45397fc39362bb0ec5bfe45e07ab3938af1c7571685506e636bced530): per-
request policy
```

9.3.9 FPT_FLS.1

Invocation of integrity test failures with preservation of secure state

/var/log/ltm.log will have the following log

```
        Jul 13 02:51:25 localhost.localdomain err fips_monitor[18833]: 01da0011:3: SelfTest/Integrity test
failure detected, triggering reboot action
```

Invocation of failures for DRBG failure

```
        Oct 10 19:52:28 bigip1.localdomain notice fault_monitord: DRBG Check Failed
```

Invocation of failures for external audit server not available failure

```
        Oct 10 19:52:28 bigip1.localdomain debug fault_monitord[8657]: 01d70003:7: Local audit server is
down checking for Remote auditing.
```

```
        Oct 10 19:52:28 bigip1.localdomain error fault_monitord[8657]: 01d70002:6: External audit server pool status is down, hence moving to degraded mode.
        Oct 10 19:52:28 bigip1.localdomain info fault_monitord[8657]: 01d70002:6: Enable maintenance mode
```

9.3.10 FPT_KST_EXT.2

All attempts to use the TOE's embedded CA's private signing key, and [selection, assignment [other secret and private keys], no other]

Private keys cannot be exported in CC / STIP mode from the WebUI

```
        Oct 8 11:01:21 amber-mgmt info tmm1[28830]: 01260005:6: /Common/ssloT_transp.app/ssloT_transp-cssl-vhf: Private key of /Common/default.crt is accessed to forge certificate for SSL forward proxy CA on TCP 10.10.11.7:43093 -> 104.22.34.105:443 (SID 4f6259e4f3b69d58d64a200cfb1ee5010a7291d651c6554ae678ce030bee7550).
```

9.3.11 FPT_RCV.1

Invocation of failures for integrity test failure

Logs can be viewed in /var/log/secure

```
secure:Sep 12 06:56:50 localhost.localdomain emerg FIPS Integrity Check::
secure:BIG-IP Integrity Check Report
secure:Integrity Check Result: [ FAIL ]
```

Resumption of regular operation after entering maintenance mode

Before the resumption of the regular service journalctl will have the following logs

```
        Jul 13 02:52:03 localhost.localdomain f5-sysinit[1620]: System was rebooted due to FIPS error in previous boot.
        Jul 13 02:52:03 localhost.localdomain f5-sysinit[1620]: Allowing recovery from FIPS error.
```

/var/log/secure will have the following log on resumption of service after failure

```
    Jul 13 02:56:53 localhost.localdomain notice FIPS Integrity Check:: Startup integrity check successful.
```

10 Appendix: Sample Secure Remote Syslog Configuration

NOTE: The following sample configuration assumes that VLANs and self-IPs have already been set up. The pool names, IP addresses, keys, and other command variables in the commands below should be replaced by names and addresses specific to your configuration. This sample is for guidance only.

In order to configure secure logging to an external syslog server, we need to configure a local SSL-to-server virtual server to encrypt the TCP Syslog traffic generated by the BIG-IP's logging systems. This virtual server will target traffic to a pool containing the IP address and port of the remote secure syslog server. We will send traffic from our High-Speed-Logging system as well as the standard syslog service to this virtual server. The High-Speed-Logging system requires a pool to target, so we will create a pool containing the IP address and port of the local encrypting virtual server. These are all base level configuration items, so they will need to be configured on each BIG-IP in the cluster, using the appropriate IP addresses, keys, and certificates for each BIG-IP, although they will all be sending traffic to the one remote secure syslog server. We will create the configuration objects in order, from the secure syslog server back to the syslog and High-Speed-Logging system, so each object in the chain is available when we configure the enclosing /calling object.

Ensure that you've imported a CA bundle (below referred to as the: "**F5secureLoggingCA_bundle.ca**" file) and the appropriate client certificate and key (matching the hostname of your DUT) to each of your BIG-IPs, then create a pool containing the IP address and TCP port of the logging network interface on the remote secure syslog server (note that each of these commands is entered as a single command line, we've added newlines for readability):

```
# create ltm pool pool_remote_secure_syslog {
    members replace-all-with { 10.89.179.1:6514 { address 10.89.179.1 } }
    monitor tcp_half_open
  }
```

Next, we create a non-floating, encrypting, SSL-to-server virtual server, utilizing that BIG-IP's key and certificate, on a private VLAN, targeting that pool on each BIG-IP. Note that the IP addresses used on the private VLAN are arbitrary, non-routable, and all the BIG-IPs in the cluster use the same IP addresses, so they each have an identical encrypting virtual server. This is because the syslog configuration is synchronized across all BIG-IPs in the cluster and it only contains one IP/port to send syslog messages.

On BIG-IP 1, execute the following TMSH commands:

```
# create ltm profile server-ssl profile_serverssl_syslog-1 {
    ca-file F5secureLoggingCA_bundle.crt
    cert b3-1.logging.f5cc.com.crt
    defaults-from serverssl
    key b3-1.logging.f5cc.com.key
    peer-cert-mode require
    authenticate-name vm179.logging.f5cc.com
  }
```

```
#  create net vlan vlan_securelog
#  create net self 10.254.216.1/24 vlan vlan_securelog
#  create ltm virtual-address 10.254.216.100
     traffic-group traffic-group-local-only
     auto-delete false
#  create ltm virtual vs_secure_syslog_target-1 {
     destination 10.254.216.100:514
     ip-protocol tcp
     pool pool_remote_secure_syslog
     profiles replace-all-with { profile_serverssl_syslog-1 tcp }
     vlans replace-all-with { vlan_securelog }
     vlans-enabled
   }
```

and on BIG-IP 2:

```
#  create ltm profile server-ssl profile_serverssl_syslog-2 {
     ca-file F5secureLoggingCA_bundle.crt
     cert b3-2.logging.f5cc.com.crt
     defaults-from serverssl
     key b3-2.logging.f5cc.com.key
     peer-cert-mode require
     authenticate-name vm179.logging.f5cc.com
   }
#  create net vlan vlan_securelog
#  create net self 10.254.216.1/24 vlan vlan_securelog
#  create ltm virtual-address 10.254.216.100
     traffic-group traffic-group-local-only
     auto-delete false
#  create ltm virtual vs_secure_syslog_target-2 {
     destination 10.254.216.100:514
     ip-protocol tcp
     pool pool_remote_secure_syslog
     profiles replace-all-with { profile_serverssl_syslog-2 tcp }
     vlans replace-all-with { vlan_securelog }
     vlans-enabled
   }
```

Then, because some of the older audit log messages do not use the High-Speed-Logging system, we modify the BIG-IP's local syslog server to send audit data to the encrypting virtual server. This configuration item is synchronized across the BIG-IPs so it does not need to be entered twice:

```
#  modify sys syslog {
     include `
       destination d_to_secure_syslog { network(\”10.254.216.100\” port(514) transport(tcp)); };
       log { source(s_syslog_pipe); filter(f_audit);    destination(d_to_secure_syslog); };
       log { source(s_syslog_pipe); filter(f_authpriv); destination(d_to_secure_syslog); };
       log { source(s_syslog_pipe); filter(f_apm);      destination(d_to_secure_syslog); };
       log { source(s_syslog_pipe); filter(f_sso);      destination(d_to_secure_syslog); };
     `
   }
```

Now, for High-Speed-Logging (HSL), we create a pool containing the IP address and TCP port of the encrypting, SSL-to-server virtual servers (one pool for both BIG-IP secure syslog target virtual servers, the pool automatically selects the proper local virtual to use):

```
#  create ltm pool pool_syslog_encryptor {
     members replace-all-with {
        10.254.216.100:514 { address 10.254.216.100 }
     }
     monitor tcp_half_open
   }
```

Next, we create an HSL remote-high-speed-log destination targeting the pool:

```
#  create sys log-config destination remote-high-speed-log hsldest_to_encryptor {
     pool-name pool_syslog_encryptor
   }
```

Then, in order to get the syslog timestamp and other identifying information included with each log message, we create an HSL remote-syslog destination targeting the remote-high-speed-log:

```
#  create sys log-config destination remote-syslog hsldest_syslog {
     format rfc5424
     remote-high-speed-log hsldest_to_encryptor
   }
```

Now, we create an HSL publisher, which will send the selected audit logging messages to both the internal syslog server (for local logging) as well as the HSL destination we just created:

```
#  create sys log-config publisher hslpub_secure_remote_syslog {
     destinations replace-all-with {
       hsldest_syslog
       local-syslog
     }
   }
```

Next, we create HSL filters to select log messages and send them through the chain to the secure remote syslog server:

```
#  create sys log-config filter hslfilter_packet_filter {
     publisher hslpub_secure_remote_syslog
     source packet_filter
   }
#  create sys log-config filter hslfilter_ssl {
     publisher hslpub_secure_remote_syslog
     source ssl
   }
#  create sys log-config filter hslfilter_tamd {
     publisher hslpub_secure_remote_syslog
     source tamd
   }
#  create sys log-config filter hslfilter_tmsh {
     publisher hslpub_secure_remote_syslog
     source tmsh
   }
```

Finally, if we are testing a system with APM provisioned (ADC-AP), then we'll enable APM syslog logging and add several additional HSL filters:

```
#  modify sys db log.access.syslog value enable
# create sys log-config filter remote_apm_filter {
    level info
    publisher hslpub_secure_remote_syslog
    source accesscontrol
  }
# create sys log-config filter remote_acl_filter {
    level info
    publisher hslpub_secure_remote_syslog
    source apmacl
  }
# create sys log-config filter remote_sso_filter {
    level info
    publisher hslpub_secure_remote_syslog
    source sso
  }
```