Exabeam Security Management Platform Supplemental Administrative Guidance for Common Criteria

Version 1.0
July 26, 2019

Exabeam, Inc.
2 Waters Park Dr., Suite 200
San Mateo, CA 94403

Prepared By:

Booz | Allen | Hamilton

delivering results that endure

Cyber Assurance Testing Laboratory
1100 West Street
Laurel, MD 20707

Contents

1 Introduction

The Target of Evaluation (TOE) is the Exabeam Security Management Platform (SMP) which includes the EX3000 and EX4000 models together as a distributed TOE. The TOE's software version is Core (PLT-i10) which includes the Data Lake (EX3000), and Advanced Analytics and Incident Responder (EX4000) software. These TOE allows a Security Administrator to access each TOE component locally with a monitor and keyboard, remote CLI via SSH, and a GUI via TLS/HTTPS. The TOE was evaluated against the requirements defined in the Exabeam Security Management Platform Security Target.

The Exabeam Security Management Platform's primary functionality is to collect network traffic and events, correlate the data collected to detect threats, and provide recommendations for responses to safeguard the network against cyberattacks. The SMP model with the Data Lake software provides the capability to collect the network traffic and events and will send that data to the other TOE component over TLS for threat detection and response recommendation. The SMP model receiving the collected events has the Advanced Analytics software which will detect threats and the Incident Responder software that will create response actions that the network administrator can perform to mitigate the threat. The TOE was evaluated as a network device only and the SMP's network traffic collection, threat detection, and threat mitigation capabilities described above were not assessed during this evaluation. The TOE is the general network device functionality (I&A, auditing, security management, trusted communications, etc.) of the SMP, consistent with the claimed Protection Profile.

As a Common Criteria evaluated product, this guidance serves to define the 'evaluated configuration' in which the evaluation was performed and to summarize how to perform the security functions that were tested as part of the evaluation.

2 Intended Audience

This document is intended for administrators responsible for installing, configuring, and/or operating the SMP. Guidance provided in this document allows the reader to deploy the product in an environment that is consistent with the configuration that was evaluated as part of the product's Common Criteria (CC) testing process. It also provides the reader with instructions on how to exercise the security functions that were claimed as part of the CC evaluation. The reader is also expected to be familiar with the general operation of the SMP product. This supplemental guidance includes references to Exabeam's standard documentation set for the product and does not explicitly reproduce materials located there.

The reader is also expected to be familiar with the Exabeam Security Management Platform Security Target and the general CC terminology that is referenced in it. This document references the Security Functional Requirements (SFRs) that are defined in the Security Target document and provides instructions for how to perform the security functions that are defined by these SFRs. The SMP product as a whole provides a great deal of security functionality but only those functions that were in the scope of the claimed PP are discussed here. Any functionality that is not described here or in the Exabeam Security Management Platform Security Target was not evaluated and should be exercised at the user's risk.

3 Terminology

In reviewing this document, the reader should be aware of the terms listed below.

CC: stands for Common Criteria. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use.

SFR: stands for Security Functional Requirement. An SFR is a security capability that was tested as part of the CC process.

TOE: stands for Target of Evaluation. This refers to the aspects of the SMP product that contain the security functions that were tested as part of the CC evaluation process.

Security Administrator: The claimed Protection Profile defines a Security Administrator role that is authorized to manage the TOE and its data. For the TOE, this is considered to be the Exabeam user for the local or remote CLI, the root user for the local CLI, and any user with the permissions provided to the 'Administrator' role for the GUI.

4 References

The following security-relevant documents are included with the TOE. This is part of the standard documentation set that is provided with the product. Documentation that is not related to the functionality tested as part of the CC evaluation is not listed here.

[1] Exabeam Appliance Setup Guide Gen 2 EX2000 & EX4000
[2] Exabeam Appliance Setup Guide EX3000

The following document was created in support of the Exabeam Security Management Platform CC evaluation:

[3] Exabeam Security Management Platform Security Target, Version 1.0

5 Evaluated Configuration of the TOE

This section lists the components that have been included in the TOE's evaluated configuration, whether they are part of the TOE itself, environmental components that support the security behavior of the TOE, or non-interfering environmental components that were present during testing but are not associated with any security claims:

5.1 TOE Components

The TOE is the Exabeam Security Management Platform (SMP), which consists of the Exabeam SMP EX3000 and EX4000 models. The following table describes the TOE components in the evaluated configuration:

Component	Definition
EX3000	Model with the Data Lake software installed

EX4000	Model with the Advanced Analytics and Incident Responder software installed

Table 1: Evaluated Components of the TOE

The hardware of the TOE is defined in the following table:

Model Number	EX3000	EX4000
Size	1 RU	1 RU
Power	AC	AC
Processor	Intel Xeon E5-2620	Intel Xeon E5-2690
Memory (RAM)	192GB DDR4 2666MHz (6 x 32GB)	256GB DDR4 2400MHz (8 x 32GB)
Storage	• 9x Seagate EC3.5v5 4TB SATA 512E 6Gbps SATA3 7200rpm 128MB 3.5i • 2x Samsung PM863a 1.92TB SSD • 1x Intel S4500 240GB SSD • Maximum Storage Capacity: 35.6TiB • Maximum Usable Capacity: 27.5TiB	• 1x Intel S3500 150GB SSD • 3x Samsung PM863A 960GB SSD • 6x Seagate EC2.5 2TB HDD

Table 2: Exabeam Hardware

The TOE's software version is Core (PLT-i10) which includes the Data Lake (EX3000), and Advanced Analytics and Incident Responder (EX4000) software. The underlying software of the TOE runs on CentOS 7.6 and includes the OpenSSL 6.0 cryptographic module.

5.2 Supporting Environmental Components

The following table lists components and applications in the environment that the TOE relies upon in order to function properly:

OE Component	Definition
Management Workstation	Any general-purpose computer that is used by an administrator to manage the TOE. For the TOE to be managed remotely the management workstation is required to have: • Browser to access the TOE's GUI • SSHv2 client to access the TOE's secure shell command-line interface The TOE's secure shell command line interface can also be accessed locally with a physical connection to the TOE using a keyboard and monitor.
Syslog Server	The TOE connects to a syslog server to send syslog messages for remote storage via TLS connection where the TOE is the TLS client. This is used to send copies of audit data to be stored in a remote location for data redundancy purposes.
OCSP Responder	A server deployed within the Operational Environment which confirms the validity and revocation status of certificates.

Table 3: Supporting Components of the Operational Environment

5.3 Assumptions

In order to ensure the product is capable of meeting its security requirements when deployed in its evaluated configuration, the following conditions must be satisfied by the organization, as defined in the claimed Protection Profile:

- **Physical security:** The SMP product does not claim any sort of physical tamper-evident or tamper-resistant security mechanisms. Therefore, it is necessary to deploy the product in a locked or otherwise physically secured environment so that it is not subject to untrusted physical modification.
- **Limited functionality:** The SMP product must only be used for its intended networking purpose. General purpose computing applications, especially those with network-visible interfaces, may compromise the security of the product if introduced.
- **No through traffic protection:** The security boundary of the Common Criteria evaluation is limited to traffic flowing to or from the TOE. The intent is for SMP to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the network device, destined for another network entity, is not covered by the NDcPP. It is assumed that this protection will be covered by cPPs for particular types of network devices (e.g., firewall).
- **Trusted administration:** The SMP product does not provide a mechanism to protect against the threat of a rogue or otherwise malicious administrator. Therefore, it is the responsibility of the organization to perform appropriate vetting and training for security administrators prior to granting them the ability to manage the product.
- **Regular updates:** SMP provides regular product updates for the SMP product that include bug fixes as well as functionality and security enhancements. It is expected that administrators are reasonably diligent in ensuring that software patches are applied regularly as they are made available.
- **Secure admin credentials:** SMP protects the administrator's credentials stored on SMP that are used to access it.
- **Components running:** It is the responsibility of the administrator to check, as appropriate, the availability of all TOE components and that the audit functionality is running properly on all TOE components to reduce the risk of an undetected attack on (or failure of) one or more TOE components.
- **Residual information:** It is the responsibility of the administrator to ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

6 Secure Acceptance, Installation, and Configuration

The process for how to order and acquire the TOE is provided under the Contact link on the Exabeam website, www.exabeam.com. Section 5.1 of this document lists the properties that are associated with the TOE. When receiving delivery of the TOE, this documentation should be checked as part of the acceptance procedures so that the correctness of the hardware can be verified.

Physical installation and first-time setup of each TOE component can be accomplished by following the procedures outlined in [1] and [2].

NOTE: Document [1] also describes the EX2000 model of SMP which is not part of the TOE.

NOTE: Documents [1] and [2] both state that the monitor and keyboard are not needed after initial installation of the TOE. These resources comprise the local CLI interface that was evaluated and can be used for local administration of the TOE.

6.1 Installation Guide

The following procedures must be completed for the initial installation of each TOE component:

1. Plug in the Kickstart USB.
2. Power on the TOE component.
3. Boot from the USB drive by pressing F11. It will take you to a boot menu - select the USB drive.
4. Press Enter at the splash screen and count down (or let the countdown go).
5. The appliance will run the automated install. When the installation is complete, the TOE component will reboot. Remove the USB drive before the installation process gets to the boot loader.
6. The appliance will boot from the hard drive.
7. Authenticate to the local CLI with 'exabeam' (Exabeam user) and the password: Welcome2Exabeam!!
    a. Do not use the root account as part of the installation process
8. Perform the Network Configuration steps per the guidance in [1] and [2].
9. Download the *./Exabeam_*<Package Name>*.PLATFORM_PLT-i##_##.EXA_SECURITY_*<Security Version>*.sxb* version that will be installed (where PLT-i## is the software version). Place it anywhere on the TOE component except /opt/exabeam_installer.
10. Change the permission of the file using the following command:
    chmod +x ./Exabeam_*<Package Name>.PLATFORM_PLT-i##_##.EXA_SECURITY_*<Security Version>*.sxb*
11. Execute the following command:
    screen –LS CC
12. Execute the following command:
    ./Exabeam_*<Package Name>.PLATFORM_PLT-i##_##.EXA_SECURITY_*<Security Version>*.sxb fresh_install*
13. The script will then guide the Exabeam user through the deployment process. The following selections must be made for the TOE to be installed in the evaluated configuration. The selection is the same for both TOE components, unless otherwise stated.
    a. Which product(s) do you wish to add?
        i. On EX4000, select *uba cm*
        ii. On EX3000, select *dl*
    b. How many nodes do you wish to add? Select *1*
    c. What is the IP address of node 1 (localhost/127.0.0.1 not allowed)? Enter <TOE component IP address>
    d. What are the roles of node 1?

i. On EX4000, select *uba_master*
ii. On EX3000, there is no selection for this step

e. Do you have a ssh private key? Select *n*
f. What's the user name used to deploy the public ssh key? Enter *Exabeam*
g. Does Exabeam need password to log in to all hosts? Select *1*
h. What's the server to synchronize time with? Select *none*
i. Would you like to add any DNS servers? Select *y*
j. What is the IP address of the DNS server? Enter <DNS server IP address>
k. Would you like to override the default docker BIP/CIDR? Select *n*
l. Would you like to override the default docker_gwbridge IP/CIDR? Select *n*
m. Would you like to override the overlay_network_subnet IP/CIDR? Select *n*
n. Do you want to use an external Certificate Authority (CA)? Select *1*
o. Do you want disaster recovery? Select *n*

14. Please wait approximately 20-30 minutes for installation to finish.
15. Run the following command:
    /opt/exabeam_installer/init/exabeam-multinode-deployment.sh --actions deploy
16. Change the default Exabeam user and root passwords using Section 7.4.
    a. The default password of the Exabeam user is:
    Welcome2Exabeam!!
    b. The default password of the root user is:
    7zMcHBZj46%EfEx!BWzs
17. The installation process is completed.

6.1.1 Firewall Rules

On both TOE components, the Security Administrator must perform the following actions:

1. Authenticate to the local CLI as the root user
2. Execute the following commands:
   firewall-cmd --get-active-zones # Get firewall zone
   firewall-cmd --zone=exabeam --add-port=2513/tcp --permanent # Make sure to use correct firewall zone, once installed Exabeam software, the active zone will be named "exabeam", otherwise "public"
   firewall-cmd --zone=exabeam --add-port=2514/tcp --permanent
   firewall-cmd --zone=exabeam --add-port=2515/tcp --permanent
   firewall-cmd --zone=exabeam --add-port=20514/tcp --permanent
   firewall-cmd --zone=exabeam --add-port=20514/udp --permanent
   firewall-cmd –reload

6.2 Power-On Self Tests

Each TOE component performs its own Power-On Self Tests (POSTs) and will report on the results of the POST through only their own mechanisms. The POSTs performed are the same for both TOE components. Upon the startup of a TOE component, all POSTs are executed, and additionally continuous conditional tests are performed while the TOE operates. Upon boot, each TOE component will check the integrity of its firmware and software images. The firmware and software images are hashed, and the hash

values are checked against a local registry of SHA-256 values for each firmware and software image. If the values match, the boot process continues to proceed. If at any time the mismatch occurs, the boot process stops, and the TOE component will enter an error state.

Additionally, the TOE's cryptographic module will test its integrity using an HMAC-SHA-256 whenever the device is restarted. The integrity test verifies that the module has not been compromised and ensures that the results of the entropy mechanism are reliable. When a self-test fails the cryptographic module will go into a hard error state. Further cryptographic operations are prevented until the error state is cleared; which will occur when the TOE component is powered off and then powered back on again, causing the cryptographic module to be reloaded.

The cryptographic module performs a DRBG Known Answer Test (KAT), where a calculated value is compared to a stored value to verify correct operation, together with a Continuous Random Number Generator Test (CRNGT), which compares the current generated value with the previous generated value. This test ensures consecutive random numbers do not repeat. If the DRBG does repeat numbers, it will restart. However, the DRBG will only produce the same output if it is given the same inputs twice which would require a statistical anomaly to occur based upon the calculated entropy rate defined in the proprietary Entropy Analysis Report provided to NIAP. In addition, DRBG health tests are performed as required by SP 800-90 section 11.

These self-tests are sufficient to validate the correct operation of the TSF because they verify that the TOE component's firmware and software images have been unmodified through integrity checks and the TOE component's cryptographic module is operating correctly. The POSTs prevent the TOE component's software from executing in an unpredictable or inconsistent manner.

NOTE: In the event that a POST fails, the TOE component will need to be rebooted. If a TOE component has been corrupted or the hardware has failed such that rebooting will not resolve the issue, a Security Administrator will need to contact Exabeam support per the guidance in Section 10.

6.3 SSH Server Configuration

Each TOE component acts as an SSH server for remote CLI management of that TOE component. In the evaluated configuration, an access control list (ACL) of IP addresses allowed for remote administration and denying access to all other IP addresses is required. This ACL must be configured using the procedures defined in https://wiki.centos.org/HowTos/Network/IPTables.

In the evaluated configuration, the TOE has a set of algorithms and configuration settings for SSH Server that must be used. The Exabeam user must verify that the configuration settings are correct on each TOE component and if necessary, modify its SSH Server configuration by performing the following actions:

1. Authenticate to the local CLI as the root user
2. Open the /etc/ssh/sshd_config file with an editor
3. Verify and/or correct the configuration settings for the following lines:

   Ciphers aes256-cbc
   HostKeyAlgorithms ssh-rsa
   MACs hmac-sha2-256,hmac-sha2-512
   KexAlgorithms diffie-hellman-group14-sha1

RekeyLimit 512M 1800
LogLevel DEBUG3

4. Save the changes to the /etc/ssh/sshd_config file
5. Executed the following command:
   sudo systemctl reload sshd

NOTE: The MAC algorithms defined above are the only ones included in the evaluated configuration and thus, the "none" MAC algorithm is never allowed for SSH.

NOTE: The diffie-hellman-group14-sha1 key exchange method defined above is the only one included in the evaluated configuration. No other key exchange methods are allowed.

NOTE: The SSH session key thresholds for time and amount of transmitted data are not configurable in the evaluated configuration. The TOE has been configured to rekey before one hour has elapsed or one gigabyte of data has been transmitted using a key; whichever occurs first. No other configuration is allowed.

NOTE: After performing an update, the Security Administrator must validate that the SSH server configuration has not changed.

NOTE: The local and remote CLI are differentiated based upon the Security Administrator's method of access (keyboard/mouse vs SSH). All management functionality of the CLI is available from both interfaces. After the configuration of the SSH server per the procedures above, the TOE's CLI can be access remotely. Therefore, the term CLI when not prefaced with local or remote means that management activity can be performed via either interface in the evaluated configuration.

6.4 Certificate Management

The TOE uses X.509v3 certificates to support authentication for internal and external TLS communication. For internal communication between EX3000 and EX4000, EX3000 and EX4000 will verify their counterpart's certificate as part of mutual authentication. For external, the EX3000 and the EX4000 will verify the Syslog Server's certificate.

During the initial deployment steps performed in Section 6.1, each TOE component generates Certification Requests for several services on the TOE component and stores them in the /opt/exabeam_installer/certs/host1/ directory under a directory for each service. If the Security Administrator needs to create another Certification Request after the initial deployment, this can be accomplished by executing the following command:

openssl req -new -sha256 -config
/opt/exabeam_installer/certs/host1/<SERVICE>/<SERVICE>*.cnf -out*
/opt/exabeam_installer/certs/host1/<SERVICE>/<SERVICE>*.csr -keyout*
/opt/exabeam_installer/certs/host1/<SERVICE>*/key.pem -nodes -newkey rsa:2048*

The Security Administrator shall perform the following actions on each TOE component for each service's Certification Request:

1. Authenticate to the CLI as the Exabeam user

2. Set the Common Name for the TOE Component by modifying the CN field in the /opt/exabeam_installer/certs/host1/<SERVICE>/<SERVICE>.cnf file
3. Copy the <service>.csr file to a removable media
4. Transfer the file to the Certificate Authority for signature
5. Copy the cert.pem and ca.pem to the /opt/exabeam_installer/certs/host1/<SERVICE>/ directory
6. Execute the following command to validate the signed certificate

openssl verify -CAfile ca.pem cert.pem

NOTE: The signed certificates MUST be named cert.pem and MUST be in .pem format.

NOTE: The Certificate Authority certificate chain MUST be named ca.pem and MUST contain the entire certificate chain from the service's cert.pem to the Certificate Authority.

The Exabeam user can delete the reference to the certificate's private key by running the 'rm' command via the CLI against the .pem file. The Exabeam user would perform this action before generating a new certificate.

6.5 TLS Server Configuration

The TOE when acting as a TLS server will only support the TLSv1.2 protocol, and will support the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246

The TOE denies all connections from clients requesting connections dependent on the following SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1 protocols. Each TOE component is a TLS server to connect and secure the following trusted paths and inter-TOE communication:

EX3000 is a TLS server for:

- management via the GUI (HTTPS/TLS)

EX4000 is a TLS server for:

- management via the GUI (HTTPS/TLS)
- receiving collected network event data for EX3000 (TLS with mutual authentication)

In the evaluated configuration, the TOE has a set of protocols, algorithms and configuration settings for operating as a TLS Server that must be used. The Exabeam user must verify that the configuration settings are correct on each TOE component and if necessary, modify its TLS Server configuration.

6.5.1 TOE Component as a Web Server for GUI

On both TOE components, the Security Administrator must perform the following actions:

1. Authenticate to the CLI as the Exabeam user
2. Open the /opt/exabeam/config/common/web/custom/application.conf file with an editor
3. Verify, correct, and/or add the configuration settings for the following lines:

webcommon.service.ciphers =[
"TLS_RSA_WITH_AES_128_CBC_SHA256",
"TLS_RSA_WITH_AES_256_GCM_SHA384",
"TLS_DHE_RSA_WITH_AES_128_CBC_SHA256",
"TLS_DHE_RSA_WITH_AES_256_CBC_SHA256",
]

4. Save the changes to the /opt/exabeam/config/common/web/custom/application.conf file
5. Execute the following commands:

web-common-stop
web-common-start

6.5.2 EX4000 as TLS Server for EX3000

On the EX4000, the Security Administrator must perform the following actions:

1. Authenticate to the CLI as the root user
2. Open the /etc/stunnel/stunnel.conf file with an editor
3. Verify, correct, and/or add the configuration settings for the following lines:

sslVersion = all
options = NO_SSLv2
options = NO_SSLv3
options = NO_TLSv1
options = NO_TLSv1.1

chroot = /var/run/stunnel
setuid = root
setgid = root
pid = /stunnel.pid
debug = 7
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1

[EX3000_to_EX4000_receiver]
cert = <TOE_certificate_chain>*.pem*
key = <TOE_certificate_key>*.pem*
CAfile = <CA_trust_store>*.pem*
OCSPaia = yes
ciphers = AES128-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256
requireCert = yes
verifyChain = yes
checkHost = <TOE_client_component_DNSname>
client = no
accept = 0.0.0.0:2515

connect = 127.0.0.1:2514
TIMEOUTbusy = 10
TIMEOUTclose = 10
TIMEOUTconnect = 10
TIMEOUTidle = 10

4. Save the changes to the /etc/stunnel/stunnel.conf file
5. Execute the following command: *systemctl restart stunnel*

NOTE: Setting the *checkHost* = <TOE_client_component_DNSname> variable defines the expected identifier to be used for the purposes of validation of the EX3000's certificate.

6.6 TLS Client Configuration

The TOE when acting as a TLS client will only support the TLSv1.2 protocol, and will support the following ciphersuites:

- TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246

Each TOE component is a TLS client to connect and secure the following trusted channels and inter-TOE communication:

EX3000 is a TLS client for:

- sending collected network event data to EX4000 (FCS_TLSC_EXT.2)
- transferring audit data to a syslog server (FCS_TLSC_EXT.1)

EX4000 is a TLS client for:

- transferring audit data to a syslog server (FCS_TLSC_EXT.1)

In the evaluated configuration, the TOE has a set of protocols, algorithms and configuration settings for operating as a TLS Client that must be used. The Exabeam user must verify that the configuration settings are correct on each TOE component and if necessary, modify its TLS Client configuration.

6.6.1 TOE Component to Syslog Server

Each TOE component stores its audit records in its own rsysreceived.log. Simultaneously, in the evaluated configuration each TOE component sends its audit records securely to a Syslog Server over TLS which occurs in real-time. In the evaluated configuration, only one Syslog Server can be configured on each TOE component. Each TOE component handles its own audit processes and does not receive audit records from the other TOE component.

On both TOE components, the Security Administrator must perform the following actions:

1. Authenticate to the CLI as the root user
2. Open the /etc/stunnel/stunnel.conf file with an editor
3. Verify, correct, and/or add the configuration settings for the following lines:

sslVersion = all
options = NO_SSLv2
options = NO_SSLv3
options = NO_TLSv1
options = NO_TLSv1.1

chroot = /var/run/stunnel
setuid = root
setgid = root
pid = /stunnel.pid
debug = 7
socket = l:TCP_NODELAY=1
socket = r:TCP_NODELAY=1

[<ExabeamModel>*_to_audit_sender]*
OCSPaia = yes
CAfile = <CA_trust_store>.pem
ciphers = AES128-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256
requireCert = yes
verifyChain = yes
checkHost = <audit_server_DNSname>
client = yes
accept = 127.0.0.1:2513
connect = <audit_server_IP>*:2515*
TIMEOUTbusy = 10
TIMEOUTclose = 10
TIMEOUTconnect = 10
TIMEOUTidle = 10

4. Save the changes to the /etc/stunnel/stunnel.conf file
5. Execute the following command: *systemctl restart stunnel && systemctl restart rsyslog*

NOTE: Setting the *checkHost* = <peer_DNSname> variable defines the reference identifier to be used for the purposes of validation of the Syslog Server's certificate.

The Syslog Server that is receiving each TOE component's audit records must support the syslog and TLSv1.2 protocols, support at least one of the four ciphersuites listed at the beginning of Section 6.6.1, and have its TLS Server certificate signed by the same Certificate Authority as the one used by the TOE component.

Since syslog functions in a streaming fashion, a communications outage between a TOE component and Syslog Server will result in audit data only being recorded locally on that TOE component. No special action needs to be taken in the event of a communications outage; no data will be transmitted without encryption and transmissions will automatically resume once communications have been re-established.

6.6.2 EX3000 as TLS Client to EX4000

NOTE: If all other prior procedures in Section 6 have been completed, the following steps will enable the communication channel between the EX3000 and EX4000 TOE components.

On the EX3000, the Security Administrator must perform the following actions:

1. Authenticate to the CLI as the root user
2. Open the /etc/stunnel/stunnel.conf file with an editor
3. Verify, correct, and/or add the configuration settings for the following lines:

   [EX3000_to_EX4000_sender]
   cert = <TOE_certificate_chain>*.pem*
   key = <TOE_certificate_key>*.pem*
   CAfile = <CA_trust_store>*.pem*
   OCSPaia = yes
   ciphers = AES128-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256
   requireCert = yes
   verifyChain = yes
   checkHost = <TOE_server_component_DNSname>
   client = yes
   accept = 127.0.0.1:2514
   connect = <TOE_server_component_IP>*:2515*
   TIMEOUTbusy = 10
   TIMEOUTclose = 10
   TIMEOUTconnect = 10
   TIMEOUTidle = 10

4. Save the changes to the /etc/stunnel/stunnel.conf file
5. Execute the following command: *systemctl restart stunnel*

NOTE: Setting the *checkHost* = <TOE_server_component_DNSname> variable defines the reference identifier to be used for the purposes of validation of the EX4000's certificate.

NOTE: The actual enablement step for the joining of the EX3000 to the TOE is the definition of the EX4000's IP address by completing the *connect* = <TOE_server_component_IP>*:2515* configuration line in step 3 above.

To disable the EX3000 from being part of the TOE, the steps 1 through 5 above will also be performed but the configuration settings in step 3 must either be removed and/or commented out of the /etc/stunnel/stunnel.conf file. Specifically, the removal of the *connect* = <TOE_server_component_IP>*:2515* configuration line is the disablement step.

The EX3000 will initiate a TLS connection to EX4000 when collected network event data is ready to be sent. If there is a communication outage between the TOE components, the collected network event data will remain on the EX3000. No special action needs to be taken in the event of a communications outage; no data will be transmitted without encryption and transmissions will automatically resume once communications have been re-established.

6.7 Cryptographic Configuration Notice

The administrator installing the TOE is expected to perform all of the operations in Section 6 of this document. This will result in the TOE components' cryptographic operations being limited to the claims made within the Common Criteria evaluation. There is no further configuration required on the TOE components' cryptographic engines as the TOE already comes pre-configured to meet many of the Common Criteria requirements, and the remaining Sections of 6.3 through 6.7 have the Security Administrator manually configuring the remaining items (i.e. ciphersuites, algorithms). For this reason, no further administrative action is required for other claimed cryptographic operations.

NOTE: The use of other cryptographic engines and cryptographic settings were not evaluated nor tested during the Common Criteria evaluation of the TOE.

NOTE: There are no known instances where key destruction does not happen as defined by the Security Target [3].

6.8 Audit Configuration

6.8.1 Configuring Auditable Events

On both TOE components, the Security Administrator must perform the following actions:

1. Authenticate to the CLI as the root user
2. Open the /etc/audit/rules.d/audit.rules file with an editor
3. Verify, correct, and/or add the configuration settings for the following lines:

```
## First rule - delete all
-D

## Increase the buffers to survive stress events.
## Make this bigger for busy systems
-b 8192

## Set failure mode to syslog
#-f 1

-a exit,always -F arch=b64 -F euid=0 -S execve -k rootact
-a exit,always -F arch=b32 -F euid=0 -S execve -k rootact
-a exit,always -F arch=b64 -F euid=1000 -S execve -k exabeamact
-a exit,always -F arch=b32 -F euid=1000 -S execve -k exabeamact

-w /etc/systemd/system/stunnel.service -p w -k stunnel_config
-w /etc/stunnel/ -p w -k stunnel_config
-w /etc/stunnel/stunnel.conf -p w -k stunnel_config
-w /etc/rsyslog.d/ -p w -k rsyslog_config
-w /etc/rsyslog.conf/ -p w -k rsyslog_config
-w /etc/rsyslog.d/exabeam_rsyslog.conf -p w -k rsyslog_config
```

-w /etc/profile.d/autologout.sh -p w -k timeout
-w /home/exabeam/.bash_logout -p w -k timeout
-w /root/.bash_logout -p w -k timeout
-w /opt/exabeam/config/custom/truststore.jks -p w -k certificate_truststrore
-w /etc/systemd/system/exabeam-web-common.service -p w -k certificate_truststore
-w /etc/audit/rules.d/audit.rules -p w -k audit_records
-w /etc/audit/auditd.conf -p w -k audit_records
-w /etc/ssh/ -p w -k ssh_config
-w /opt/exabeam_installer/group_vars/all.yml -p w -k banner_config
-w /etc/issue -p w -k banner_config
-w /etc/issue.net -p w -k banner_config
-w /opt/exabeam/config/common/web/custom/application.conf -p w -k web_services_config
-w /opt/exabeam/config/common/eds/custom/application.conf -p w -k web_services_config
-w /etc/security/pwquality.conf -p w -k pw_config

4. Save the changes to the /etc/audit/rules.d/audit.rules file
5. Execute the following command: *systemctl daemon-reload && service auditd restart*
6. Open the /home/exabeam/.bash_logout file with an editor
7. Verify, correct, and/or add the configuration settings for the following lines:

```
#!/bin/bash
# ~/.bash_logout
lastcommand=$(history | cut -c 8- | tail -n 1 | sed -e 's/^[ \t]*//g' | sed -e 's/[ \t]*$//g')
echo lastcommand is: “$lastcommand”
username=$(whoami)
if [ "$lastcommand" = "exit" ] || [ "$lastcommand" = "logout" ]; then
echo "User ${username} exit." | systemd-cat -t bash_logout -p info
else
echo "Idle timeout for user ${username}, audit log recorded." |
systemd-cat -t bash_logout -p warning
fi
echo Clean bash history
history -c
echo "" > ~/.bash_history
```

8. Save the changes to the /home/exabeam/.bash_logout file
9. Open the /root/.bash_logout file with an editor
10. Verify, correct, and/or add the configuration settings for the following lines:

```
#!/bin/bash
# ~/.bash_logout
lastcommand=$(history | cut -c 8- | tail -n 1 | sed -e 's/^[ \t]*//g' | sed -e 's/[ \t]*$//g')
echo lastcommand is: “$lastcommand”
username=$(whoami)
```

if ["$lastcommand" = "exit"] || ["$lastcommand" = "logout"]; then
echo "User ${username} exit." | systemd-cat -t bash_logout -p info
else
echo "Idle timeout for user ${username}, audit log recorded." |
systemd-cat -t bash_logout -p warning
fi
echo Clean bash history
history -c
echo "" > ~/.bash_history

11. Save the changes to the /root/.bash_logout file

The audit functionality starts automatically with the TOE's boot up process. In the evaluated configuration, the audit functions of the TOE are provided by rsyslog and the audit functions can be enabled or disabled by the root user on the local CLI using the following commands:

systemctl start rsyslog
systemctl stop rsyslog

NOTE: After performing an update, the Security Administrator must validate that the auditable event configuration has not changed.

6.8.2 Configuring Audit Storage

The maximum allocated space for rsysreceived.log is 21GB. The rsysreceived.log function has 2 log files and each log file's size is 10.5GB. When both audit log files are full, rsysreceived.log will roll the audit log files by deleting the archived log file, turning the active log file into the archived file, and creating a new active log file for rsysreceived.log; to which new audit records are written.

On both TOE components, the Security Administrator must perform the following actions:

1. Authenticate to the CLI as the root user
2. Open the /etc/rsyslog.d/exabeam_rsyslog.conf file with an editor
3. Verify, correct, and/or add the configuration settings for the following lines to the top of the file:

 # Provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

 # Provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

module(load="imtcp")
input(type="imtcp" port="2514" address="127.0.0.1")

#action(type="omfile" file="/var/log/rsysreceived.log")
$outchannel log_rotation, /var/log/rsysreceived.log, 10485760000,
/etc/rsyslog.d/log_rotation_script

. :omfile:$log_rotation*

4. Save the changes to the /etc/rsyslog.d/exabeam_rsyslog.conf file
5. Open the /etc/rsyslog.d/log_rotation_script file with an editor
6. Verify, correct, and/or add the configuration setting for the following line:

   mv /var/log/rsysreceived.log /var/log/rsysreceived.log.1

7. Save the changes to the /etc/rsyslog.d/log_rotation_script file

Only the Exabeam user (local and remote CLI) and root user (local CLI only) can delete the audit logs using the 'rm' command and only the root user (local CLI only) can modify the audit logs. This is enforced by the TOE's permissions assigned to its users and what management activities can be performed over its interfaces.

Local audit logs for a TOE component can be read through the local and remote CLI by entering the following command:

less /var/log/rsyslogreceived.log

6.9 Verify Software Version

Once the TOE is physically installed and all configuration actions are performed in Section 6 of this document, it is recommended that a Security Administrator acquire the software image for the currently distributed version from Exabeam and perform a software upgrade to the latest version. Depending on when each TOE component was manufactured, they may have an older software version initially installed on them. The procedures for performing a secure software update can be found in Section 7.8.

7 Secure Management of the TOE

The following sub-sections provide information on managing TOE functionality that is relevant to the claimed Protection Profile. All functions described in this section apply to both TOE components.

7.1 Authenticating to the TOE

Each TOE component performs the same user authentication functionality. Users can authenticate to a TOE component via its CLI or GUI. The CLI can be accessed remotely through an SSH client or locally with a monitor and keyboard. The GUI can be accessed remotely through a web browser and is protected by HTTPS/TLS.

The CLI can be accessed remotely through an SSH client or locally with a monitor and keyboard. The local CLI requires the user to authenticate to the TOE's local authentication mechanism with their username/password combination and will grant access when the credentials match those stored on the TOE. The remote CLI is protected by SSH and allows users to authenticate against the TOE's local authentication mechanisms with either their username/password combination or SSH public key and will grant access when the credentials match those stored on the TOE. The SSH client must support the following:

- Transport encryption algorithms: aes256-cbc
- Public key authentication algorithm: ssh-rsa

- Data integrity MAC algorithms: hmac-sha2-256 and/or hmac-sha2-512
- Key exchange method: diffie-hellman-group14-sha1

SSH public/private key pairs must be generated and have the public key loaded on the TOE so that SSH authentication using a public-key is possible. Perform the following steps to add an authorized public-key to the Exabeam user on the TOE:

1. On the Management Workstation with the SSH client, generate a new public/private key pair
2. Export the public key using OpenSSH format
3. Authenticate to the remote CLI as the Exabeam user
4. Open the .ssh/authorized_keys file with an editor
5. Paste the public key in the file
6. Save the .ssh/authorized_keys file

The GUI can be accessed through a Security Administrator entering the GUI's URL https://[TOE_IP_ADDRESS]:8484 in their web browser. The web browser must support TLSv1.2 and at least one of the ciphersuites supported by the GUI which are defined in Section 6.5 of this document. The GUI allows users to authenticate with their username/password combination against the TOE's local authentication mechanism and will grant access when the credentials match those stored on the TOE.

7.2 Failed Authentication Lockout

Both the EX3000 and EX4000 have GUI and remote CLI interfaces. In the evaluated configuration, the TOE will lock a remote administrative account when an administrator configured number of successive invalid login attempts have been made.

The TOE maintains a counter per username for the number of failed authentication attempts and tracks the time when each failed authentication attempt occurs. If a valid password is provided before the failed attempt threshold value is met, then authentication is granted and the counter resets to zero. If the limit of failed authentication attempts is reached, the account associated with the username will be locked. Once an account is locked, repeated attempts to authenticate with that account will result in displaying the following error message:

- GUI:

```
Number of wrong login attempts exceeded. Your account is
locked. Please contact your Exabeam administrator.
```

- Remote CLI:

```
Permission denied (publickey,keyboard-interactive).
lins-macbook-pro:host1-08-22 lin$ ssh exabeam@192.168.168.74
************************************************************
*****
* This system is for the use of authorized users only.
    *
************************************************************
*****
Account temporarily locked due to 3 failed logins
(2 minutes left to unlock)
```

The user associated with an offending account will be locked out and no authentication attempts will be approved until a Security Administrator manually unlocks the account (remote CLI and GUI accounts) or

alternatively, for only a remote CLI account, it can also be unlocked once the lockout time period is reached.

7.2.1 Configure Lockout Policy for CLI Users

The CLI lockout policy includes the number of failed authentication attempts before the user's account is locked and the length of time before the account is unlocked. A locked CLI user can be unlocked by a Security Administrator or by reaching the time period before the account is unlocked. To configure the lockout policy for CLI users, perform the following procedures:

1. Authenticate to the CLI as the Exabeam user
2. Open the /opt/exabeam_installer/group_vars/all.yml file with an editor
3. Verify, correct, and/or add the configuration settings for the following lines:

   login_attempts: <Value between 1 and 20>
   lockout_period_seconds: <Value between 120 and 10,800 seconds>

4. Save the /opt/exabeam_installer/group_vars/all.yml file
5. Run the following commands to redeploy:

   screen -LS CC
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh --actions deploy

NOTE: The root account via the local CLI is not subject to lockout due to authentication failures and thus, authentication failures by remote Security Administrators cannot lead to a situation that prevents all administration of the TOE.

7.2.2 Configure Lockout Policy for GUI Users

The GUI lockout policy includes the number of failed authentication attempts before the user's account is locked. A locked GUI user must be unlocked by a Security Administrator. To configure the lockout policy for CLI users, perform the following procedures:

1. Authenticate to the CLI as the Exabeam user
2. Open the /opt/exabeam/config/common/web/custom/application.conf file with an editor
3. Verify, correct, and/or add the configuration setting for the following line:
   webcommon.auth.failedLoginLockout = <Value between 1 and 20>
4. Save the /opt/exabeam/config/common/web/custom/application.conf file
5. Restart the web service by executing the following commands:
   web-common-stop && web-common-start

7.2.3 Unlock Locked User Account

The Security Administrator can unlock a user's locked account by performing the following procedures:

Remote CLI

1. Authenticate to the local CLI as the root user
2. Execute the following command:
   faillock --user <Locked username> *--reset*

GUI

1. Authenticate to the CLI as the Exabeam user
2. Execute the following commands:

   source /opt/exabeam/bin/shell-environment.bash
   mongo exabeam_user_db --eval 'db.exabeam_user_collection.remove({"_id": "<Locked username>*"})'*

A GUI user with Administrator privileges can also unlock another GUI account by resetting the offending account's password. For directions in resetting a user's GUI account password, refer to Section 7.4.3.

7.3 User Accounts and User Management

There are two types of user accounts on each TOE component, those that access the TOE through the CLI, and those that access through the GUI. The CLI can be accessed locally through a keyboard and monitor or remotely through an SSH session. The GUI can only be accessed remotely. The only administrative action allowed before authentication is the ability to view the security banner for the GUI and the CLI. All further management of the TOE and its TSF data is limited based upon the TOE's authentication mechanisms, the available user accounts on each interface, and the access control policies.

The Exabeam user provides the majority of the management of the TOE security functions and is the only Security Administrator for the remote CLI. For the local CLI, the Exabeam user is the primary Security Administrator but there is also the root account which can perform the entire set of security functions which are available to the Exabeam user. Thus, in all cases where the Security Target states the Exabeam user can perform a function, the root user can also perform that function. The root user can also perform additional audit management functions, unlock the Exabeam user account due to failed authentication attempts, configure the reference and/or expected identifiers on the TOE components, and cannot have its account become locked. The TOE's CLI access control policies differentiate these functions between the Exabeam user and root user roles. The Exabeam user has the ability to assume the role of root to perform management activities. It is recommended that the Exabeam user always be used over the root account for management.

The GUI has users, which can belong to one or more roles and the TOE enforces a role-based access control (RBAC) policy based upon the role(s) assigned to a user. Each role defines a set of permissions and the permissions that can perform TSF functionality are 'Manage Users and Context Sources' and 'Manage Context Tables'. The default role with these permissions is the 'Administrator' role but the TOE allows the definition of new roles with these permissions by a user with the 'Administrator' role. Therefore, any user with the 'Administrator' role or any role created with one or both of these permissions is considered a Security Administrator. The GUI also has a default user account called the 'Admin' user which belongs to the 'Administrator' role and has the default password *changeme*. The 'Admin' user is forced to have their default password changed after their first authentication to the TOE component. However, the 'Admin' user cannot change its name and the 'Administrator' role cannot have its permissions changed.

7.4 Password Management

The GUI and the CLI on each TOE component has password-based authentication and the passwords can be composed of any combination of upper and lower case letters, numbers and special characters. The

accepted special characters for both the GUI and the CLI are: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, and “).” In order to minimize the risk of account compromise, it is recommended to use a password that includes a mixture of uppercase, lowercase, numeric, and special characters and is not a common word or phrase but is not so complex that it must be written down in order to be remembered.

7.4.1 Configuring Password Length

Passwords for the CLI have a minimum password length between 5 characters and 15 characters in the evaluated configuration. The minimum password length for the CLI can be configured by performing the following procedures:

1. Authenticate to the CLI as the root user
2. Open the /etc/pam.d/password-auth file with an editor
3. Verify, correct, and/or add the configuration setting for the following line:

   password requisite pam_pwquality.so minlen=<MINIMUM_PASSWORD_LENGTH> enforce_for_root dcredit=-1 ucredit=-1 ocredit=-1 lcredit=0 try_first_pass local_users_only retry=3 authtok_type=

4. Save the /etc/pam.d/password-auth file
5. Repeat steps 2 through 4 for the following files:
   /etc/pam.d/password-auth-ac
   /etc/pam.d/system-auth
   /etc/pam.d/system-auth-ac

For the GUI, the minimum password length is between 1 and 15 characters and can be configured by performing the following procedures:

1. Authenticate to the CLI as the Exabeam user
2. Open the /opt/exabeam/config/common/web/custom/application.conf file with an editor
3. Verify, correct, and/or add the configuration setting for the following line:

   webcommon.auth.passwordConstraints.minLength = 15

4. Save the /opt/exabeam/config/common/web/custom/application.conf file
5. Executed the following command:

   web-common-stop && web-common-start

7.4.2 Changing Passwords for CLI Users

To change a CLI password for a user, perform the following procedures:

1. Authenticate to the CLI as the user
2. Executed the following commands:

   sudo passwd <User’s username>

3. Enter the user’s new password value (performed twice)

7.4.3 Changing Passwords for GUI Users

To change a CLI password for a user, perform the following procedures:

1. Authenticate to the GUI as the user
2. Navigate to Settings page via the cog icon
3. Click on “User Management” > “Users”.
4. Click on the icon “reset password” icon next to the user’s username that will have their password changed
5. In the password and confirm password fields, input the new password and then click “OK”

NOTE: The GUI has a default user account called the ‘Admin’ user which belongs to the ‘Administrator’ role and is required to have its default password changed after the user’s initial authentication.

7.5 Login Banner

When authenticating locally or remotely to either TOE component, the pre-authentication banner is displayed prior to authentication.

7.5.1 CLI Banner

On both TOE components, the Security Administrator can set the banner for the local and remote CLI by performing the following actions:

1. Authenticate to the CLI as the Exabeam user
2. Open the /opt/exabeam_installer/group_vars/all.yml file with an editor
3. Modify the “BannerText:” tag by adding the banner text that will be displayed (example below)
4. Save the /opt/exabeam_installer/group_vars/all.yml file
5. Execute the following commands to commit the configuration changes to the system:

   screen -LS CC
   /opt/exabeam_installer/init/exabeam-multinode-deployment.sh --actions deploy

6. Select the option “Nuke existing services and deploy” and wait for deployment to complete

NOTE: In the example below, note the >> at the beginning of each line of banner text. These indicate the mandatory two spaces that must be at the beginning of each line.

BannerText: |

>>**

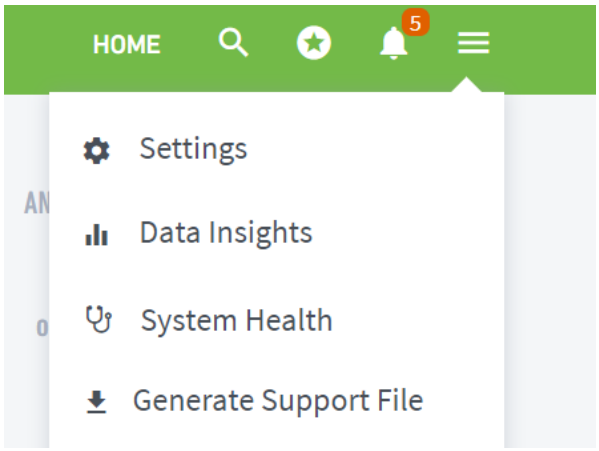
>>* This system is for the use of authorized users only. *

>>**

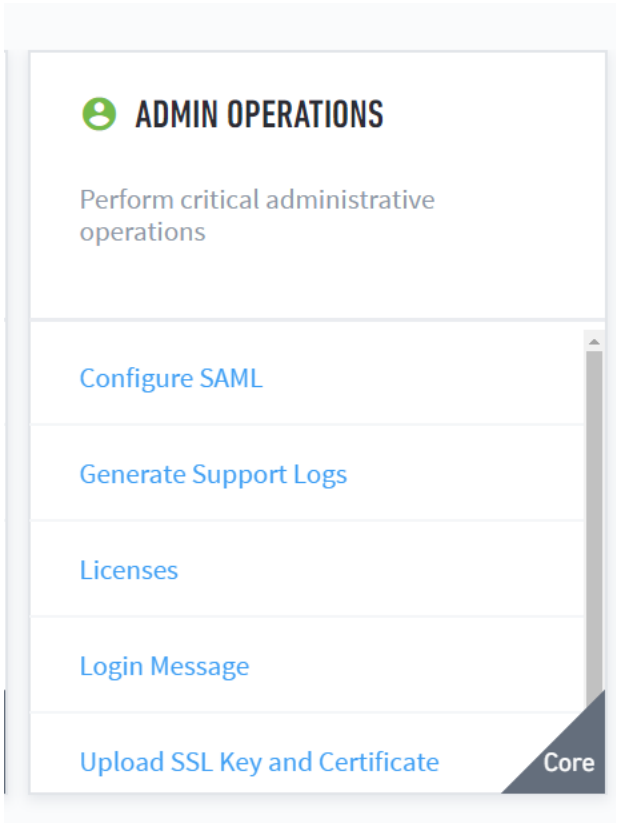
7.5.2 GUI Banner

On both TOE components, the Security Administrator can set the banner for the GUI by performing the following actions:

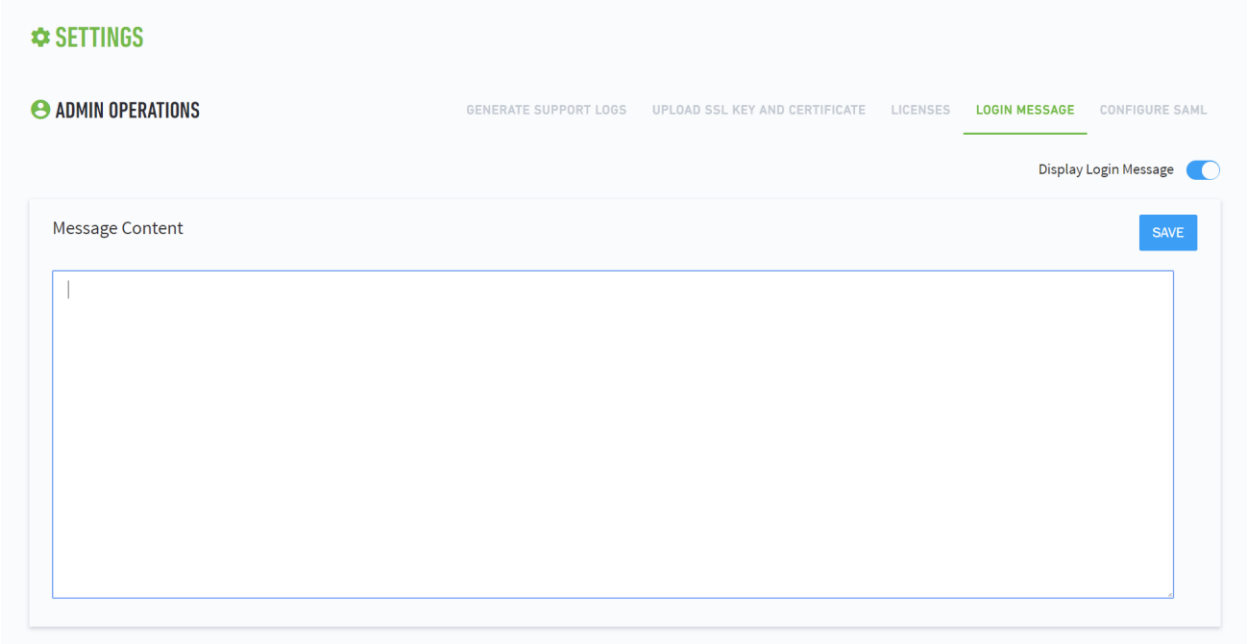
1. Authenticate to the GUI as a Security Administrator
2. Select **Settings**



3. Under **Admin Operations**, select **Login Message**



4. Toggle **Display Login Message** to **On** and edit the message as desired. Press **Save**.



7.6 Session Termination

7.6.1 Admin Logout

Any user accessing the TOE via the CLI or the GUI can terminate their own session. On the GUI, EX3000 has 'Logout' button and EX4000 has a 'Sign Out' button. For the local and remote CLI, the Exabeam user can terminate their own session by using the 'exit' command on both the EX3000 and EX4000.

7.6.2 Termination from Inactivity

A maximum inactivity time period for a session can be configured for each management interface. When the maximum time period of inactivity is reached, the management interface's session will be terminated.

CLI Sessions

On both TOE components, the Security Administrator can set the inactivity time period for the local and remote CLI by performing the following actions:

1. Authenticate to the CLI as the root user
2. Open the /etc/profile.d/autologout.sh file with an editor
3. Set the 'TMOUT' variable to a value between 1 to 36,000 seconds (default 7,200 seconds)
4. Save the /etc/profile.d/autologout.sh file

NOTE: It is recommended to not set the 'TMOUT' variable to a value less than 60 seconds.

GUI Sessions

On both TOE components, the Security Administrator can set the inactivity time period for the GUI by performing the following actions:

1. Authenticate to the CLI as the Exabeam user
2. Open the /opt/exabeam/config/common/web/custom/application.conf file with an editor
3. Set the 'webcommon.silhouette.authenticator.cookieIdleTimeout' variable to a value between 60 to 86,400 seconds (default 7,200 seconds)
4. Save the /opt/exabeam/config/common/web/custom/application.conf file
5. Execute the following commands:

   web-common-stop
   web-common-start

7.7 System Time Configuration

Each TOE component has an underlying hardware clock that is used for time keeping. In the evaluated configuration of the TOE, the system time is expected to be manually set on each TOE component by an Exabeam user via the local or remote CLI by performing the Linux *date* command. Refer to the Linux man page for use and options for the *date* command.

It is recommended that the Exabeam user set the time on both TOE components as close as possible. The Exabeam user will also need to record the offset between the TOE components; so that the audit records when correlated from both TOE components can be related based upon the time offset. The Exabeam user via the local or remote CLI will execute the following command on the EX4000 to record the offset:

sudo clockdiff <EX3000 IP address>

The Exabeam user must perform this activity every time either TOE component's system time is set and when a TOE component is rebooted. It is also recommended to check the offset periodically to determine if there is any further variance between the TOE components.

7.8 Secure Updates

To maintain security throughout the lifecycle of the SMP product, the TOE provides a mechanism to apply software updates. The Security Administrator is made aware of new updates to the TOE by Exabeam sending an email with a link to an Exabeam hosted FTP server to download the latest software. The Security Administrator can also access Exabeam's website to check for the latest software version as well as contact customer support to request the latest software version.

The Security Administrator can determine the currently executing version of each TOE component by performing the following procedures:

1. Authenticate to the GUI as a Security Administrator
2. Click on the menu icon in the top right corner of the GUI
3. Examine the current version number at the bottom of the drop-down menu

When updating the software version for the EX4000 and EX3000, it is recommended to apply the update on the EX4000 first and then the EX3000. In the evaluated configuration, prior to performing a software update on either TOE component, the Exabeam user must perform the disablement step in Section 6.6 to disconnect the TOE components. Once both TOE components have had the software update applied, the enablement step in Section 6.6 will be performed to join the TOE components again.

The following procedures can be performed on both TOE components to install a software update:

1. The new version of the TOE component's software is downloaded to the Management Workstation
2. The Security Administrator will retrieve from their email a file with the SHA-256 hash value for the entire software installer package (i.e. both header script and payload)
3. Authenticate to the remote CLI as the Exabeam user
    a. Do not use the root account as part of the update process
4. Check available disk space on the system, execute the command: *df -h*
    a. Recommended 25% or more free space available for each individual disk
5. SCP push (over SSH) the software installer package from the Management Workstation to the TOE component
    a. Place it anywhere on the TOE component except /opt/exabeam_installer
6. SCP push the corresponding hash file for the installer package from the Management Workstation to the TOE component
    a. Must be in the same directory as the software installer package
7. In the directory where the software installer package and hash file are stored, execute the following command:
    sha256sum -c checksums.txt
8. The output of this command will be either OK or FAILED
    a. If FAILED is received Exabeam user must abort the installation process and contact Exabeam support per the guidance in Section 10
    b. If OK, the installation process will continue
9. Initiates the installation process by executing the following command:
    ./<UpgradePackage>.sxb upgrade
10. The TOE component will then verify a SHA-256 hash within the header script of the installer package against the payload during initial extraction of the installer package
    a. If the hash value is missing or the comparison does not result in a match, the installation will abort immediately and the Exabeam user will need to contact Exabeam support per the guidance in Section 10
    b. If the comparison does match, the installer runs to update the TOE component's software
11. Once the update process is complete:
    a. If successful, the TOE component's software version will be the version associated with the update, and an audit record of the successful update will be generated
    b. If there is an error, the TOE component's software version will be the same version before the update process began, and the TOE will output the error

NOTE: If the update fails due to error, the Exabeam user will need to contact Exabeam support per the guidance in Section 10. Errors that can occur are the disk space being full, disk failure, and loss of network connectivity for the SSH connection.

NOTE: After an update, the Security Administrator must validate the configuration settings defined in Section 6 (i.e. SSH server configuration, auditable event configuration) to ensure that the TOE is still in its evaluated configuration.

The security mechanisms that support continuous proper functioning of the TOE during an update depend on the services being upgraded as part of the update. In the case of a TOE component requiring a reboot as part of the update, services and security mechanisms will not be available during reboot. During the

software update process, a TOE component's services and security mechanisms that are available depend on the functionality that is being changed during the software update. As each service and its security mechanisms are being updated, access to the services is disabled in a secure manner.

8 Auditing

In order to be compliant with Common Criteria, the TOE components audit the events in the table below. Performing the steps in Sections 6.3 and 6.8 of this document are all the steps required for the TOE to generate the required audit records, store them locally, and send them to a remote Syslog Server.

Sample audit records for each security-relevant auditable event are included in the following table.

EX 3000	EX 4000	Auditable Events	Sample Audit Record
X	X	Start-up and shut-down of the audit functions	**Start-up of the audit functions** Jul 10 17:03:56 <toe_component> systemd[1]: Starting System Logging Service... Jul 10 17:03:56 <toe_component> rsyslogd[24700]: [origin software="rsyslogd" swVersion="8.24.0-34.el7" x-pid=" Jul 10 17:03:56 <toe_component> systemd[1]: Started System Logging Service. **Shut-down of the audit functions** Jul 10 17:09:04 <toe_component> systemd[1]: Stopping System Logging Service... Jul 10 17:09:04 <toe_component> rsyslogd[24700]: [origin software="rsyslogd" swVersion="8.24.0-34.el7" x-pid=" Jul 10 17:09:04 <toe_component> systemd[1]: Stopped System Logging Service.
X	X	Administrative login and logout	**Local CLI Login** Jun 12 23:24:15 <toe_component> common-criteria-sshd: Jun 12 23:24:06 <toe_component> login: pam_unix(login:session): session opened for user <username> by LOGIN(uid=0) Jun 12 23:24:15 <toe_component> common-criteria-sshd: Jun 12 23:24:06 <toe_component> login: LOGIN ON tty1 BY <username> **Local CLI Logout** Oct 12 14:58:14 <toe_component> login: pam_unix(login:session): session closed for user <username> **Remote CLI Login** Jun 12 23:10:17 <toe_component> common-criteria-sshd: Jun 12 23:10:13 <toe_component> sshd[6156]: Accepted publickey for <username> from <ip> port <port> ssh2: RSA SHA256:iuJMgN+DzsclqsM0vTWTHQv5qoJ13wbPFj6+qknQqx4 **Remote CLI Logout**

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Apr 10 16:27:28 <toe_component> bash_logout: User <username> exit. Apr 10 16:27:28 <toe_component> sshd[15680]: pam_unix(sshd:session): session closed for user <username> Apr 10 16:27:28 <toe_component> systemd-logind: Removed session 354. **GUI Success** Jun 12 21:56:51 <toe_component> common-criteria-app-audit: 2019-06-12 21:56:43.770 l= INFO User [<username>] has been successfully logged in from <ip> class=com.exabeam.webcommon.controllers.LoginController thread=play-akka.actor.default-dispatcher-50 **GUI Failure Logout** Apr 10 16:30:16 <toe_component> common-criteria-app-audit: 2019-04-10 20:30:11.587 l= INFO User <username> has been logged out class=com.exabeam.webcommon.controllers.AuthController$ thread=play-akka.actor.default-dispatcher-3
X	X	Changes to TSF data related to configuration changes	**Local/Remote CLI Configuration Change** Apr 10 12:35:29 <toe_component> common-criteria-sys-audit: type=SYSCALL msg=audit(1554917726.519:113981): arch=c000003e syscall=59 success=yes exit=0 a0=2178960 a1=2161830 a2=215a280 a3=7ffe9c2b6060 items=2 ppid=21962 pid=34477 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=112 comm="vi" exe="/usr/bin/vi" key=(null) Apr 10 12:35:29 <toe_component> common-criteria-sys-audit: type=EXECVE msg=audit(1554917726.519:113981): argc=2 a0="vi" a1="/etc/profile.d/autologout.sh" Apr 10 12:35:29 <toe_component> common-criteria-sys-audit: type=CWD msg=audit(1554917726.519:113981): cwd="/home/exabeam" Apr 10 12:35:29 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1554917726.519:113981): item=0 name="/bin/vi" inode=137374 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 **GUI Configuration Change** Mar 28 14:27:51 <toe_component> common-criteria-access: 2019-03-28 19:27:47,455 method=POST uri=/api/setup/loginBanner?_=1553801267341 remote-address=<remote_user_ip> status=200 time=15ms user-agent=[Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko] exabeam-app-user-name=admin Mar 28 14:27:51 <toe_component> common-criteria-audit: 2019-03-28 19:27:47.439 l=TRACE Http request received by netty: DefaultHttpRequest(chunked: false)

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Mar 28 14:27:51 <toe_component> common-criteria-audit: POST /api/setup/loginBanner?_=1553801267341 HTTP/1.1 Mar 28 14:27:51 <toe_component> common-criteria-audit: Content-Type: application/json; charset=UTF-8 Mar 28 14:27:51 <toe_component> common-criteria-audit: Accept: */* Mar 28 14:27:51 <toe_component> common-criteria-audit: X-Requested-With: XMLHttpRequest Mar 28 14:27:51 <toe_component> common-criteria-audit: Referer: https:// <toe_ip>:<port>/settings Mar 28 14:27:51 <toe_component> common-criteria-audit: Accept-Language: en-US Mar 28 14:27:51 <toe_component> common-criteria-audit: Accept-Encoding: gzip, deflate Mar 28 14:27:51 <toe_component> common-criteria-audit: User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Mar 28 14:27:51 <toe_component> common-criteria-audit: Host: <toe_ip>:<port> Mar 28 14:27:51 <toe_component> common-criteria-audit: Content-Length: 105 Mar 28 14:27:51 <toe_component> common-criteria-audit: Connection: Keep-Alive Mar 28 14:27:51 <toe_component> common-criteria-audit: Cache-Control: no-cache Mar 28 14:27:51 <toe_component> common-criteria-audit: Cookie: ssid=f9f32bd3f38855ecbb05c9ca1a6f1d876c45107efcdd008d99f63db8adaa530e720670bc03aff4f112cc5fdd1e2b9747bf3534f5989beb9c8ea8ae60ab3e57964f4f77bec51012990c4fde0dc58818b17412f50d5e91d826ec151c0f2c2179dd44531c1183bcfb52590cb4c876455cc54de4abc0ffca82927c6e3d5b6c9b31fc; ExabeamAppUserName=admin class=play thread=New I/O worker #38 Mar 28 14:27:51 <toe_component> common-criteria-audit: 2019-03-28 19:27:47.440 l=TRACE Serving this request with: <function1> class=play thread=New I/O worker #38 Mar 28 14:27:51 <toe_component> common-criteria-audit: 2019-03-28 19:27:47.441 l=TRACE Parsing AnyContent as json class=play thread=play-akka.actor.default-dispatcher-40 Mar 28 14:27:51 <toe_component> common-criteria-audit: 2019-03-28 19:27:47.443 l=TRACE Invoking action with request: POST /api/setup/loginBanner?_=1553801267341 class=play thread=play-akka.actor.default-dispatcher-37
X	X	Generating/import of, changing, or deleting of cryptographic keys	Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=SYSCALL msg=audit(1556221613.900:5117786): arch=c000003e syscall=59 success=yes exit=0 a0=211fe50 a1=2128470 a2=2127990 a3=7ffd90134960 items=2 ppid=12870 pid=8048 auid=1000 uid=<user_id> gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=12756 comm="ssh-keygen" exe="/usr/bin/ssh-keygen" key="exabeamact"

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=EXECVE msg=audit(1556221613.900:5117786): argc=3 a0="ssh-keygen" a1="-f" a2="<key_identifier>" Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=CWD msg=audit(1556221613.900:5117786): cwd="/home/exabeam" Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1556221613.900:5117786): item=0 name="/usr/bin/ssh-keygen" inode=5250697 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1556221613.900:5117786): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=5245851 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
X	X	Resetting passwords	Apr 29 17:27:54 <toe_component> common-criteria-sshd: Apr 29 17:27:49 <toe_component> passwd: pam_unix(passwd:chauthtok): password changed for <username>
X	X	Enabling communications between a pair of components. Disabling communications between a pair of components.	**Enabling communications between a pair of components.** May 10 17:26:40 <toe_component> stunnel_watch.py[24758]: WARNING:root:New Stunnel connection added: {'client': 'yes', 'name': '<connection_name>', 'accept': '127.0.0.1:2514', 'connect': '<external_component_hostname/ip>:<port>'} **Disabling communications between a pair of components.** May 10 17:35:19 <toe_component> stunnel_watch.py[24758]: WARNING:root:Stunnel connection removed: {'client': 'yes', 'name': '<connection_name>', 'accept': '127.0.0.1:2514', 'connect': '<external_component_hostname/ip>:<port>'}
X	X	Failure to establish a HTTPS Session.	Jun 26 00:10:32 <toe_component> common-criteria-audit: 2019-06-27 00:10:30.537 l= WARN SSL session failure with /<ip>:<port> due to Received Finished message before ChangeCipherSpec class=play.core.server.netty.ExabeamUpstreamHandler thread=New I/O worker #25
X	X	Failure to establish an SSH session	Apr 30 15:29:04 <toe_component> common-criteria-sshd: Apr 30 15:29:04 <toe_component> sshd[16955]: error: PAM: Permission denied for <username> from <ip>
X	X	Failure to establish a TLS Session (TOE to Syslog Server)	Apr 29 12:05:53 <toe_component> stunnel[17169]: LOG5[0]: s_connect: connected <peer_ip>:<port> Apr 29 12:05:53 <toe_component> stunnel[17169]: LOG5[0]: Service [<connection_name>] connected remote server from <toe_ip>:<port>

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Apr 29 12:05:53 <toe_component> stunnel[17169]: LOG4[0]: Rejected by CERT at depth=1: C=<C>, ST=<ST>, L=<L>, O=<O>, OU=<OU>, CN=<CN> Apr 29 12:05:53 <toe_component> stunnel[17169]: LOG7[0]: TLS alert (write): fatal: unknown CA Apr 29 12:05:53 <toe_component> stunnel[17169]: LOG7[0]: Service [<connection_name>] finished (0 left)
X		Failure to establish a TLS Session (TOE to TOE)	Feb 12 11:45:11 <toe_component> stunnel: LOG5[4]: s_connect: connected <external_toe_component_ip>:<port> Feb 12 11:45:11 <toe_component> stunnel: LOG5[4]: Service [<connection_name>] connected remote server from <toe_component_ip>:<port> Feb 12 11:45:11 <toe_component> stunnel: LOG7[4]: TLS alert (write): fatal: illegal parameter Feb 12 11:45:11 <toe_component> stunnel: LOG3[4]: SSL_connect: 140920F8: error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned Feb 12 11:45:11 <toe_component> stunnel: LOG7[4]: Service [<connection_name>] finished (1 left)
X	X	Failure to establish a TLS Session (Web browser to TOE GUI)	Jun 26 00:10:32 <toe_component> common-criteria-audit: 2019-06-27 00:10:30.537 l= WARN SSL session failure with /<ip>:<port> due to Received Finished message before ChangeCipherSpec class=play.core.server.netty.ExabeamUpstreamHandler thread=New I/O worker #25
	X	Failure to establish a TLS Session (TOE to TOE)	May 02 16:19:01 <toe_component> stunnel[1386]: LOG5[0]: Service [<connection_name>] accepted connection from <external_toe_component_ip>:<port> May 02 16:19:01 <toe_component> stunnel[1386]: LOG3[0]: SSL_accept: 1408A0C1: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher May 02 16:19:01 <toe_component> stunnel[1386]: LOG7[0]: Service [<connection_name>] finished (0 left)
X	X	Unsuccessful login attempts limit is met or exceeded	Jun 13 19:59:20 <toe_component> common-criteria-sshd: Jun 13 19:59:19 <toe_component> sshd[37191]: Failed keyboard-interactive/pam for <username> from <ip> port <port> ssh2 Jun 13 19:59:20 <toe_component> common-criteria-sshd: Jun 13 19:59:19 <toe_component> sshd[37191]: error: maximum authentication attempts exceeded for <username> from <ip> port <port> ssh2 [preauth] Jun 13 19:59:20 <toe_component> common-criteria-sshd: Jun 13 19:59:19 <toe_component> sshd[37191]: Disconnecting: Too many authentication failures [preauth]
X	X	All use of the identification and authentication mechanism.	**Local CLI Success** Jun 12 23:24:15 <toe_component> common-criteria-sshd: Jun 12 23:24:06 <toe_component> login: pam_unix(login:session): session opened for user <username> by LOGIN(uid=0)

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Jun 12 23:24:15 <toe_component> common-criteria-sshd: Jun 12 23:24:06 <toe_component> login: LOGIN ON tty1 BY <username> **Local CLI Failure** Jun 12 23:25:10 <toe_component> common-criteria-sshd: Jun 12 23:25:03 <toe_component> login: FAILED LOGIN SESSION FROM tty1 FOR <username>, Permission denied **Remote CLI Success** Jun 12 23:10:17 <toe_component> common-criteria-sshd: Jun 12 23:10:13 <toe_component> sshd[6156]: Accepted publickey for <username> from <ip> port <port> ssh2: RSA SHA256:iuJMgN+DzsclqsM0vTWTHQv5qoJ13wbPFj6+qknQqx4 **Remote CLI Failure** Jun 12 23:13:56 <toe_component> common-criteria-sshd: Jun 12 23:13:54 <toe_component> sshd[25357]: Failed publickey for <username> from <ip> port 64590 ssh2: RSA SHA256:BxNH554bZLw4RUcE3KII2D4gjE3MVI3d7lD92yM4Hq0 **GUI Success** Jun 12 21:56:51 <toe_component> common-criteria-app-audit: 2019-06-12 21:56:43.770 l= INFO User [<username>] has been successfully logged in from <ip> class=com.exabeam.webcommon.controllers.LoginController thread=play-akka.actor.default-dispatcher-50 **GUI Failure** Jun 12 21:58:02 <toe_component> common-criteria-app-audit: 2019-06-12 21:57:58.301 l= INFO Failed to log in as <username> from <ip> class=com.exabeam.webcommon.controllers.LoginController thread=play-akka.actor.default-dispatcher-66
X	X	All use of the identification and authentication mechanism.	**Local CLI Success** Jun 12 23:24:15 <toe_component> common-criteria-sshd: Jun 12 23:24:06 <toe_component> login: pam_unix(login:session): session opened for user <username> by LOGIN(uid=0) Jun 12 23:24:15 <toe_component> common-criteria-sshd: Jun 12 23:24:06 <toe_component> login: LOGIN ON tty1 BY <username> **Local CLI Failure** Jun 12 23:25:10 <toe_component> common-criteria-sshd: Jun 12 23:25:03 <toe_component> login: FAILED LOGIN SESSION FROM tty1 FOR <username>, Permission denied **Remote CLI Success**

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Jun 12 23:10:17 <toe_component> common-criteria-sshd: Jun 12 23:10:13 <toe_component> sshd[6156]: Accepted publickey for <username> from <ip> port <port> ssh2: RSA SHA256:iuJMgN+DzsclqsM0vTWTHQv5qoJ13wbPFj6+qknQqx4 **Remote CLI Failure** Jun 12 23:13:56 <toe_component> common-criteria-sshd: Jun 12 23:13:54 <toe_component> sshd[25357]: Failed publickey for <username> from <ip> port 64590 ssh2: RSA SHA256:BxNH554bZLw4RUcE3KII2D4gjE3MVI3d7lD92yM4Hq0 **GUI Success** Jun 12 21:56:51 <toe_component> common-criteria-app-audit: 2019-06-12 21:56:43.770 l= INFO User [<username>] has been successfully logged in from <ip> class=com.exabeam.webcommon.controllers.LoginController thread=play-akka.actor.default-dispatcher-50 **GUI Failure** Jun 12 21:58:02 <toe_component> common-criteria-app-audit: 2019-06-12 21:57:58.301 l= INFO Failed to log in as <username> from <ip> class=com.exabeam.webcommon.controllers.LoginController thread=play-akka.actor.default-dispatcher-66
X	X	Unsuccessful attempt to validate a certificate	May 03 18:12:54 <toe_component> stunnel[48315]: LOG7[1]: Service [<connection_name>] started May 03 18:12:54 <toe_component> stunnel[48315]: LOG5[1]: Service [<connection_name>] accepted connection from <external_toe_component_ip>:<port> May 03 18:12:54 <toe_component> stunnel[48315]: LOG3[1]: error queue: 14089086: error:14089086:SSL routines:ssl3_get_client_certificate:certificate verify failed May 03 18:12:54 <toe_component> stunnel[48315]: LOG3[1]: error queue: D0C5006: error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib May 03 18:12:54 <toe_component> stunnel[48315]: LOG3[1]: error queue: 4067072: error:04067072:rsa routines:RSA_EAY_PUBLIC_DECRYPT:padding check failed May 03 18:12:54 <toe_component> stunnel[48315]: LOG3[1]: SSL_accept: 407006A: error:0407006A:rsa routines:RSA_padding_check_PKCS1_type_1:block type is not 01 May 03 18:12:54 <toe_component> stunnel[48315]: LOG7[1]: Service [<connection_name>] finished (0 left)
X	X	Unsuccessful attempt to validate a certificate	Jul 08 16:35:19 <toe_component> stunnel[12218]: LOG5[0]: s_connect: connected <peer_ip>:<port> Jul 08 16:35:19 <toe_component> stunnel[12218]: LOG5[0]: Service [<connection_name>] connected remote server from <external_toe_component_ip>:<port>

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Jul 08 16:35:19 <toe_component> stunnel[12218]: LOG7[0]: OCSP: Connected <ocsp_ip>:<port> Jul 08 16:35:19 <toe_component> stunnel[12218]: LOG3[0]: OCSP: Certificate revoked Jul 08 16:35:19 <toe_component> stunnel[12218]: LOG5[0]: OCSP: Revoked at: Jul 8 20:33:02 2019 GMT Jul 08 16:35:19 <toe_component> stunnel[12218]: LOG4[0]: Rejected by OCSP at depth=0: C=<C>, ST=<ST>, L=<L>, O=<O>, OU=<OU>, CN=<CN> Jul 08 16:35:19 <toe_component> stunnel[12218]: LOG3[0]: SSL_connect: 14090086: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed Jul 08 16:35:19 <toe_component> stunnel[12218]: LOG7[0]: Service [<connection_name>] finished (0 left)
X	X	Any attempt to initiate a manual update	Jul 11 14:11:55 <toe_component> common-criteria-sys-audit: type=SYSCALL msg=audit(1562868712.999:18343610): arch=c000003e syscall=59 success=yes exit=0 a0=1b29590 a1=1b24cd0 a2=1b49b60 a3=7ffc9f5469a0 items=3 ppid=25453 pid=26106 auid=1000 uid=<user_id> gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts7 ses=36851 comm="Exabeam_LMS_LMS" exe="/usr/bin/bash" key="exabeamact" Jul 11 14:11:55 <toe_component> common-criteria-sys-audit: type=EXECVE msg=audit(1562868712.999:18343610): argc=3 a0="/bin/bash" a1="./Exabeam_LMS_LMS-i20_128.PLATFORM_PLT-i10_196.EXA_SECURITY_c180531_96.sxb" a2="upgrade" Jul 11 14:11:55 <toe_component> common-criteria-sys-audit: type=CWD msg=audit(1562868712.999:18343610): cwd="/home/exabeam/installer" Jul 11 14:11:55 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1562868712.999:18343610): item=0 name="./Exabeam_LMS_LMS-i20_128.PLATFORM_PLT-i10_196.EXA_SECURITY_c180531_96.sxb" inode=13107619 dev=08:03 mode=0100700 ouid=1000 ogid=1000 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 Jul 11 14:11:55 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1562868712.999:18343610): item=1 name="/bin/bash" inode=5244750 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 Jul 11 14:11:55 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1562868712.999:18343610): item=2 name="/lib64/ld-linux-x86-64.so.2" inode=5245851 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 Jul 11 14:11:55 <toe_component> common-criteria-sys-audit: type=PROCTITLE msg=audit(1562868712.999:18343610): proctitle=2F62696E2F62617368002E2F4578616265616D5F4C4D535F4C4D532D6932305F3132382E504C4154464F524D5F504C542D6931305

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			F3139362E4558415F53454355524954595F633138303533315F39362E7 378620075706772616465
X	X	All management activities of the TSF	**Local/Remote CLI Management Activity** Apr 10 12:35:29 <toe_component> common-criteria-sys-audit: type=SYSCALL msg=audit(1554917726.519:113981): arch=c000003e syscall=59 success=yes exit=0 a0=2178960 a1=2161830 a2=215a280 a3=7ffe9c2b6060 items=2 ppid=21962 pid=34477 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts3 ses=112 comm="vi" exe="/usr/bin/vi" key=(null) Apr 10 12:35:29 <toe_component> common-criteria-sys-audit: type=EXECVE msg=audit(1554917726.519:113981): argc=2 a0="vi" a1="/etc/profile.d/autologout.sh" Apr 10 12:35:29 <toe_component> common-criteria-sys-audit: type=CWD msg=audit(1554917726.519:113981): cwd="/home/exabeam" Apr 10 12:35:29 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1554917726.519:113981): item=0 name="/bin/vi" inode=137374 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 **GUI Management Activity** Mar 28 14:27:51 <toe_component> common-criteria-access: 2019-03-28 19:27:47,455 method=POST uri=/api/setup/loginBanner?_=1553801267341 remote-address=<remote_user_ip> status=200 time=15ms user-agent=[Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko] exabeam-app-user-name=admin Mar 28 14:27:51 <toe_component> common-criteria-audit: 2019-03-28 19:27:47.439 l=TRACE Http request received by netty: DefaultHttpRequest(chunked: false) Mar 28 14:27:51 <toe_component> common-criteria-audit: POST /api/setup/loginBanner?_=1553801267341 HTTP/1.1 Mar 28 14:27:51 <toe_component> common-criteria-audit: Content-Type: application/json; charset=UTF-8 Mar 28 14:27:51 <toe_component> common-criteria-audit: Accept: */* Mar 28 14:27:51 <toe_component> common-criteria-audit: X-Requested-With: XMLHttpRequest Mar 28 14:27:51 <toe_component> common-criteria-audit: Referer: https:// <toe_ip>:<port>/settings Mar 28 14:27:51 <toe_component> common-criteria-audit: Accept-Language: en-US Mar 28 14:27:51 <toe_component> common-criteria-audit: Accept-Encoding: gzip, deflate Mar 28 14:27:51 <toe_component> common-criteria-audit: User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Mar 28 14:27:51 <toe_component> common-criteria-audit: Host: <toe_ip>:<port> Mar 28 14:27:51 <toe_component> common-criteria-audit: Content-Length: 105 Mar 28 14:27:51 <toe_component> common-criteria-audit: Connection: Keep-Alive Mar 28 14:27:51 <toe_component> common-criteria-audit: Cache-Control: no-cache Mar 28 14:27:51 <toe_component> common-criteria-audit: Cookie: ssid=f9f32bd3f38855ecbb05c9ca1a6f1d876c45107efcdd008d99f63db8adaa530e720670bc03aff4f112cc5fdd1e2b9747bf3534f5989beb9c8ea8ae60ab3e57964f4f77bec51012990c4fde0dc58818b17412f50d5e91d826ec151c0f2c2179dd44531c1183bcfb52590cb4c876455cc54de4abc0ffca82927c6e3d5b6c9b31fc; ExabeamAppUserName=admin class=play thread=New I/O worker #38 Mar 28 14:27:51 <toe_component> common-criteria-audit: 2019-03-28 19:27:47.440 l=TRACE Serving this request with: <function1> class=play thread=New I/O worker #38 Mar 28 14:27:51 <toe_component> common-criteria-audit: 2019-03-28 19:27:47.441 l=TRACE Parsing AnyContent as json class=play thread=play-akka.actor.default-dispatcher-40 Mar 28 14:27:51 <toe_component> common-criteria-audit: 2019-03-28 19:27:47.443 l=TRACE Invoking action with request: POST /api/setup/loginBanner?_=1553801267341 class=play thread=play-akka.actor.default-dispatcher-37
X	X	Management of cryptographic keys	Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=SYSCALL msg=audit(1556221613.900:5117786): arch=c000003e syscall=59 success=yes exit=0 a0=211fe50 a1=2128470 a2=2127990 a3=7ffd90134960 items=2 ppid=12870 pid=8048 auid=1000 uid=<user_id> gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=12756 comm="ssh-keygen" exe="/usr/bin/ssh-keygen" key="exabeamact" Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=EXECVE msg=audit(1556221613.900:5117786): argc=3 a0="ssh-keygen" a1="-f" a2="<key_identifier>" Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=CWD msg=audit(1556221613.900:5117786): cwd="/home/exabeam" Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1556221613.900:5117786): item=0 name="/usr/bin/ssh-keygen" inode=5250697 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0 Apr 25 15:46:54 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1556221613.900:5117786): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=5245851 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
X	X	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	**EX3000 Initiation of the trusted channel** Apr 04 18:38:43 <toe_component> stunnel: LOG5[0]: s_connect: connected <external_toe_component_ip>:<port> Apr 04 18:38:43 <toe_component> stunnel: LOG5[0]: Service [<connection_name>] connected remote server from <external_toe_component_ip>:<port> Apr 04 18:38:43 <toe_component> stunnel: LOG6[0]: TLS connected: new session negotiated **EX4000 Initiation of the trusted channel** Apr 04 17:38:43 <toe_component> stunnel: LOG7[main]: Service [<connection_name>] accepted (FD=3) from <external_toe_component_ip>:<port> Apr 04 17:38:43 <toe_component> stunnel: LOG7[1]: Service [<connection_name>] started Apr 04 17:38:43 <toe_component> stunnel: LOG5[1]: Service [<connection_name>] accepted connection from <external_toe_component_ip>:<port> Apr 04 17:38:43 <toe_component> stunnel: LOG6[1]: TLS accepted: new session negotiated **EX3000 Termination of the trusted channel** Apr 04 18:40:20 <toe_component> systemd: Stopping SSL tunnel for network daemons... Apr 04 18:40:20 <toe_component> stunnel: LOG7[main]: Found 1 ready file descriptor(s) Apr 04 18:40:20 <toe_component> stunnel: LOG7[main]: FD=4 events=0x2001 revents=0x1 Apr 04 18:40:20 <toe_component> stunnel: LOG7[main]: FD=7 events=0x2001 revents=0x0 Apr 04 18:40:20 <toe_component> systemd: Stopped SSL tunnel for network daemons. **EX4000 Termination of the trusted channel** Apr 04 17:40:20 <toe_component> stunnel: LOG6[1]: TLS socket closed (SSL_read) Apr 04 17:40:20 <toe_component> stunnel: LOG7[1]: Sent socket write shutdown Apr 04 17:40:20 <toe_component> stunnel: LOG5[1]: Connection closed: 0 byte(s) sent to TLS, 7227672 byte(s) sent to socket Apr 04 17:40:20 <toe_component> stunnel: LOG7[1]: Remote descriptor (FD=8) closed Apr 04 17:40:20 <toe_component> stunnel: LOG7[1]: Local descriptor (FD=3) closed

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Apr 04 17:40:20 <toe_component> stunnel: LOG7[1]: Service [<connection_name>] finished (0 left) **EX3000 Failure of the trusted channel functions** Feb 12 11:45:11 <toe_component> stunnel: LOG5[4]: s_connect: connected <external_toe_component_ip>:<port> Feb 12 11:45:11 <toe_component> stunnel: LOG5[4]: Service [<connection_name>] connected remote server from <toe_component>:<port> Feb 12 11:45:11 <toe_component> stunnel: LOG7[4]: TLS alert (write): fatal: illegal parameter Feb 12 11:45:11 <toe_component> stunnel: LOG3[4]: SSL_connect: 140920F8: error:140920F8:SSL routines:ssl3_get_server_hello:unknown cipher returned Feb 12 11:45:11 <toe_component> stunnel: LOG7[4]: Service [<connection_name>] finished (1 left) **EX4000 Failure of the trusted channel functions** Feb 11 11:17:55 <toe_component> stunnel: LOG7[main]: Service [<connection_name>] accepted (FD=12) from <external_toe_component_ip>:<port> Feb 11 11:17:55 <toe_component> stunnel: LOG5[106]: Service [<connection_name>] accepted connection from <external_toe_component_ip>:<port> Feb 11 11:17:55 <toe_component> stunnel: LOG7[106]: TLS alert (write): fatal: handshake failure Feb 11 11:17:55 <toe_component> stunnel: LOG3[106]: SSL_accept: 1408A0C1: error:1408A0C1:SSL routines:ssl3_get_client_hello:no shared cipher Feb 11 11:17:55 <toe_component> stunnel: LOG7[106]: Service [<connection_name>] finished (2 left)
X	X	Discontinuous changes to time – either Administrator actuated or changed via an automated process.	Apr 22 13:11:14 <toe_component> sudo: <username> : TTY=pts/6 ; PWD=/home/exabeam ; USER=root ; COMMAND=/bin/date +%Y%m%d -s 20000101 Jan 1 00:00:00 <toe_component> systemd: Time has been changed Jan 1 00:00:07 <toe_component> common-criteria-sys-audit: type=SYSCALL msg=audit(1555953074.960:2433357): arch=c000003e syscall=59 success=yes exit=0 a0=5599e6581258 a1=5599e6593bf8 a2=5599e65a2990 a3=0 items=2 ppid=22582 pid=22585 auid=1000 uid=<user_id> gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts6 ses=5974 comm="date" exe="/usr/bin/date" key=(null) Jan 1 00:00:07 <toe_component> common-criteria-sys-audit: type=EXECVE msg=audit(1555953074.960:2433357): argc=4 a0="date" a1="+%Y%m%d" a2="-s" a3="20000101" Jan 1 00:00:07 <toe_component> common-criteria-sys-audit: type=CWD msg=audit(1555953074.960:2433357): cwd="/home/exabeam"

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Jan 1 00:00:07 <toe_component> common-criteria-sys-audit: type=PATH msg=audit(1555953074.960:2433357): item=0 name="/bin/date" inode=5246181 dev=08:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
X	X	Initiation of update; result of the update attempt (success or failure)	**Initiation of update; successful result of the update attempt** Apr 3 13:53:14 <toe_component> exabeam_installer: Start action: upgrade. Apr 3 13:53:41 <toe_component> exabeam_installer: Checksums verified successfully. Apr 3 14:42:22 <toe_component> exabeam_installer: Action upgrade finished. **Initiation of update; failure result of the update attempt** Apr 3 15:28:05 <toe_component> exabeam_installer: Start action: upgrade. Apr 3 15:28:32 <toe_component> exabeam_installer: Checksums don't appear to match, exiting script.
X	X	The termination of a local session by the session locking mechanism.	Apr 10 14:37:21 <toe_component> bash_logout: Idle timeout for user <username>, audit log recorded. Apr 10 14:37:21 <toe_component> login: pam_unix(login:session): session closed for user exabeam Apr 10 14:37:29 <toe_component> common-criteria-sys-audit: type=CRED_DISP msg=audit(1554921441.808:76733): pid=1401 uid=<user_id> auid=1000 ses=175 msg='op=PAM:setcred grantors=pam_securetty,pam_faillock,pam_unix acct="<username>" exe="/usr/bin/login" hostname=<toe_component> addr=? terminal=tty1 res=success' Apr 10 14:37:29 <toe_component> common-criteria-sys-audit: type=USER_END msg=audit(1554921441.809:76734): pid=1401 uid=<user_id> auid=1000 ses=175 msg='op=PAM:session_close grantors=pam_selinux,pam_loginuid,pam_selinux,pam_namespace,pam_keyinit,pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_lastlog acct="<username>" exe="/usr/bin/login" hostname=<toe_component> addr=? terminal=tty1 res=success'
X	X	The termination of a remote session by the session locking mechanism.	**Remote CLI** Apr 10 14:37:40 <toe_component> bash_logout: Idle timeout for user <username>, audit log recorded. Apr 10 14:37:40 <toe_component> sshd[15609]: pam_unix(sshd:session): session closed for user <username> Apr 10 14:37:40 <toe_component> systemd-logind: Removed session 177. **GUI**

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			Jun 11 17:56:31 <toe_component> common-criteria-app-audit: 2019-06-11 21:56:18.543 l= INFO <username>'s session has expired. remote=<ip> class=com.exabeam.webcommon.controllers.AuthController$ thread=play-akka.actor.default-dispatcher-24
X	X	The termination of an interactive session.	**Local CLI** Oct 12 14:58:14 <toe_component> login: pam_unix(login:session): session closed for user <username> **Remote CLI** Apr 10 16:27:28 <toe_component> bash_logout: User <username> exit. Apr 10 16:27:28 <toe_component> sshd[15680]: pam_unix(sshd:session): session closed for user <username> Apr 10 16:27:28 <toe_component> systemd-logind: Removed session 354. **GUI** Apr 10 16:30:16 <toe_component> common-criteria-app-audit: 2019-04-10 20:30:11.587 l= INFO User <username> has been logged out class=com.exabeam.webcommon.controllers.AuthController$ thread=play-akka.actor.default-dispatcher-3
X	X	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	**Initiation of the trusted channel** May 14 20:08:21 <toe_component> systemd[1]: Started SSL tunnel for network daemons. May 14 20:08:21 <toe_component> stunnel[10599]: LOG7[0]: Service [<connection_name>] started May 14 20:08:21 <toe_component> stunnel[10599]: LOG6[0]: s_connect: connecting <external_toe_component_ip>:<port> May 14 20:08:21 <toe_component> stunnel[10599]: LOG5[0]: s_connect: connected <external_toe_component_ip>:<port> May 14 20:08:21 <toe_component> stunnel[10599]: LOG5[0]: Service [<connection_name>] connected remote server from <toe_ip>:<port> May 14 20:08:21 <toe_component> stunnel[10599]: LOG6[0]: TLS connected: new session negotiated **Termination of the trusted channel** May 14 20:08:22 <toe_component> systemd[1]: Stopping SSL tunnel for network daemons... May 14 20:08:22 <toe_component> stunnel[10599]: LOG7[main]: Found 1 ready file descriptor(s) May 14 20:08:22 <toe_component> stunnel[10599]: LOG7[main]: FD=4 events=0x2001 revents=0x1 May 14 20:08:22 <toe_component> stunnel[10599]: LOG7[main]: FD=7 events=0x2001 revents=0x0

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			May 14 20:08:22 <toe_component> stunnel[10599]: LOG7[main]: Dispatching a signal from the signal pipe May 14 20:08:22 <toe_component> systemd[1]: Stopped SSL tunnel for network daemons. **Failure of the trusted channel functions** May 14 20:33:09 <toe_component> stunnel[18180]: LOG7[0]: TLS alert (read): fatal: handshake failure May 14 20:33:09 <toe_component> stunnel[18180]: LOG3[0]: SSL_connect: 14077410: error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure May 14 20:33:09 <toe_component> stunnel[18180]: LOG5[0]: Connection reset: 0 byte(s) sent to TLS, 0 byte(s) sent to socket May 14 20:33:09 <toe_component> stunnel[18180]: LOG7[0]: Deallocating application specific data for session connect address May 14 20:33:09 <toe_component> stunnel[18180]: LOG7[0]: Remote descriptor (FD=8) closed May 14 20:33:09 <toe_component> stunnel[18180]: LOG7[0]: Local descriptor (FD=3) closed May 14 20:33:09 <toe_component> stunnel[18180]: LOG7[0]: Service [<connection_name>] finished (0 left)
X	X	Initiation of the trusted path. Termination of the trusted path. Failures of the trusted path functions.	**CLI Initiation of the trusted path** Apr 9 14:37:42 <toe_component> common-criteria-sshd: Apr 9 14:37:42 <toe_component> sshd[2791]: Accepted keyboard-interactive/pam for exabeam from 192.168.1.181 port 56643 ssh2 Apr 9 14:37:42 <toe_component> common-criteria-sshd: Apr 9 14:37:42 <toe_component> sshd[2791]: pam_unix(sshd:session): session opened for user <username> by (uid=0) **GUI Initiation of the trusted path** Apr 9 14:39:32 <toe_component> common-criteria-app-audit: 2019-04-09 18:39:23.201 l= INFO User [<username>] has been successfully logged in class=com.exabeam.webcommon.controllers.LoginController thread=play-akka.actor.default-dispatcher-45 **CLI Termination of the trusted path** Apr 9 14:37:52 <toe_component> common-criteria-sshd: Apr 9 14:37:45 <toe_component> sshd[2791]: pam_unix(sshd:session): session closed for user <username> **GUI Termination of the trusted path** Apr 9 14:39:32 <toe_component> common-criteria-app-audit: 2019-04-09 18:39:30.238 l= INFO User <username> has been logged out class=com.exabeam.webcommon.controllers.AuthController$ thread=play-akka.actor.default-dispatcher-44

EX 3000	EX 4000	Auditable Events	Sample Audit Record
			CLI Failures of the trusted path functions Mar 26 19:48:59 <toe_component> common-criteria-sshd: Mar 26 19:48:50 <toe_component> sshd[29174]: Connection from <remote_ip> port <port> on <toe_ip> port <port> Mar 26 19:48:59 <toe_component> common-criteria-sshd: Mar 26 19:48:50 <toe_component> sshd[29174]: Failed publickey for <username> from <remote_ip> port <port> ssh2: RSA SHA256:B10XY1NWUJBfjiJrNYWraHkgMR9lEmHn0uRIX7anlLI Mar 26 19:48:59 <toe_component> common-criteria-sshd: Mar 26 19:48:50 <toe_component> sshd[29174]: Postponed keyboard-interactive for <username> from <remote_ip> port <port> ssh2 [preauth] **GUI Failures of the trusted path functions** Jun 11 02:35:52 <toe_component> common-criteria-audit: 2019-06-11 02:35:49.789 l= WARN SSL session failure with /<remote_ip>:<port> due to Invalid Padding length: 156 class=play.core.server.netty.ExabeamUpstreamHandler thread=New I/O worker #17 Jun 11 02:35:52 <toe_component> common-criteria-audit: javax.net.ssl.SSLHandshakeException: Invalid Padding length: 156

Table 4: Sample Audit Records

9 Operational Modes

When each TOE component is first installed, it is considered to be in its normal operational mode. After initial installation, the TOE must still be placed into its evaluated configuration by performing the steps described in Section 6 of this document. Once placed in the evaluated configuration, the TOE's normal operational mode will perform the functions as described in the Security Target [3].

There is no separate error mode or other degraded mode of operation. In the event that a POST fails, the TOE will need to be rebooted. If the TOE has been corrupted or the hardware has failed such that rebooting will not resolve the issue, an Administrator will need to contact Exabeam support per the guidance in Section 10.

10 Additional Support

Exabeam provides technical support for its products if needed. Customers can register for a support account at https://community.exabeam.com/login. Customer tickets are primarily created for issues through Exabeam's Community site. Additionally, customers can contact Exabeam support by calling +1 (844) 392-2326 (USA and EMEA) or +1 (877) 237-6070 (Asia Pacific).