Configuring LoadMaster for Common Criteria Conformance

Version 0.2

This document details the configuration settings that must be modified from their default values so that LoadMaster operation and behavior conforms to the Common Criteria standard.

Table of Contents

Common Criteria Configuration Instructions....3

1. Target Release....3
2. Installation Process....3
3. Operational Environment....3
4. Supported Platforms....3
5. CC Configuration Process....4

5.1 Log In....4

5.2 Set Minimum Password Length....4

5.3 System Reboot....4

5.4 System Shutdown....5

5.5 Reset Machine....5

5.6 Start-up and Self-Test....5

5.7 Logging Out....5

5.8 Admin WUI Access....6

5.9 User Creation....6

5.10 Zeroization....7

5.11 Setting Date/Time....7

5.12 Configuring NTP Server....7

5.13 Set the GUI Banner....8

5.14 Intermediate Certificate....8

5.15 Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set....9

5.16 Set ECC Ciphers for Self-Signed Certificates and Outbound Connections....10

5.17 Hash Cryptographic Operation (Hash Algorithm)....11

5.18 Keyed Hash Cryptographic Operation (Keyed Hash Algorithm)....11

5.19 Random Bit Generation....11

5.20 Generate CSR (Certificate Signing Request)....11

5.21 Auditing....13

5.22 Secure Remote Logging....14

5.23 Failed Login Attempts....15

5.24 Idle Session Timeout....15

5.25 Disable SSH Access....15

5.26 Enable OCSP Checking....16

5.27 SAN Extensions....16

5.28 Reference Identifiers 16
5.29 Using CLI 17
5.30 Set the CLI Banner 17
5.31 Disable CLI Virtual Service Administration 17
5.32 Setup Admin UI Access via LDAP 18
5.33 Lockdown Admin UI logon to Certificate Only with OCSP validation 20
5.34 Logging for Admin UI logon 20
5.35 Elliptical Curve Cipher Set 20
5.36 Installing an Update Image 20
5.37 Sample Audit Logs 21
6. References 31

Revision History

Version	Date	Changes
Version 0.1	12/16/2022	Initial Version
Version 0.2	01/19/2023	Updated after addressing ECR comments

Common Criteria Configuration Instructions

Follow the instructions in this document to install and license LoadMaster, and to make the configuration changes required after installation to bring the system into “Common Criteria mode”.
This document is a guide to the Kemp LoadMaster implementation of the Common Criteria Network Device Protection Profile v2.2e (CC-NDPP).

1. Target Release

These instructions have been prepared for **LoadMaster OS Version 7.2.48.8**, which is the Common Criteria tested, evaluated, and certified release. This release can be downloaded directly from Kemp website at: https://support.kemptechnologies.com/hc/en-us/sections/4405063394061-Latest-Firmware. If this firmware version is not available, please reach out to Kemp Support at https://support.kemptechnologies.com/hc/en-us/articles/201870787.

2. Installation Process

The only prerequisite is the deployment, licensing, and initial configuration of LoadMaster. An additional VMware platform installation document is available from the Kemp website to guide you through this process for Virtual LoadMaster. Please note the following:

- You need a console connected during the initial boot process
- After boot, you will use the console to set the IP address data for the LoadMaster
- You’ll need to create a Kemp ID to license the unit online; it’s a simple process that is confirmed via email.
- When you reach the point in the VMware platform installation document where LoadMaster is licensed, be sure to choose the **Online Licensing** option, specify the Kemp ID and password you created, and accept the license provided by the licensing server.

3. Operational Environment

The TOE supports the following hardware, software, and firmware components in its operational environment.

Component	**Usage/Purpose Description**
Management Workst	Workstation providing local console access to the TOE. Workstation providing a browser to connected to the Web User Interface (WU TLSv1.2 or TLSv1.1.
Audit Server	Syslog server that receives audit logs from the TOE over TLSv1.2 or TLSv1.1.
ESXi Server	ESXi v6.7 acting as the hypervisor for Virtual LoadMaster.
LDAP Server	Optional authentication server supporting LDAP over TLSv1.2 or TLSv1.1.
NTP Server	Optional NTP server supporting SHA-1 integrity verification.

4. Supported Platforms

Category	**Identifier**
Hardware Versions	Physical appliances: LoadMaster X15, LoadMaster X25, LoadMaster X40
Software Versions	Virtual appliance: Virtual LoadMaster Physical and virtual appliance software:

5. CC Configuration Process

Once you complete the steps in the above document, follow the steps in these sub-sections.

When administrators log in with role-based credentials, their access is limited to commands they have privileges and permissions to use based on the Common Criteria standards. No management functionality is available prior to successful identification and authentication of the users.

In an evaluated configuration, TOE supports only a trusted channel to an external audit server (a syslog server). That trusted channel must be configured to be protected by TLS.

Network management communication paths are protected against modification and disclosure by TLS.

5.1 Log In

1. **Log in to the UI** via HTTPS using the IP address assigned during installation, the ‘bal’ administrative login, and the password you specified during installation.
   a. Download the LoadMaster issuing CA RSA certificate and install it in the management workstation certificate store and/or the browser certificate store.
2. After initially logging in to the LoadMaster, if Session Management is enabled - some login information is displayed:
   a. The last login time and IP address of the current user
   b. The number of successful logins by the current user in the last 30 days
   c. The total number of failed logins attempts by any user (including unknown usernames) since the last successful login
   d. Audit Logs are generated for each action which is performed by a user; either using the API or the WUI.
3. The primary user (bal) always has full permissions. Secondary users may be restricted to certain functions.
4. Only the bal user is permitted to set the Basic Authentication password.
5. Users must be authenticated before logging on to the LoadMaster.
6. Users with the 'All Permissions' permission set can view the **Enable Session Management**, **Require Basic Authentication,** and the **Basic Authentication Password** fields. However, users with the 'All Permissions' permission set can configure the **Failed Login Attempts** and **Idle Session Timeout values**.
7. Users with the 'User Administration' permissions set can view the screen but all buttons and input fields are greyed out.
8. All other users cannot view the **WUI Session Management**, **Currently Active Users** or **Currently Blocked Users** sections of the **WUI Configuration** screen.

5.2 Set Minimum Password Length

1. In the left frame menu, click **System Configuration > System Administration > User Management** to set the desired **Minimum Password Length** (default is 8).
2. All characters which include combination of lowercase, uppercase letters, numbers, and special characters are allowed while setting the password.
3. The Minimum Password Length should be configured between 8 and 16 characters.

5.3 System Reboot

The Kemp LoadMaster network load balancer appliance can be restarted from the Web Management interface. To restart the LoadMaster:

1. In the left frame menu, click **System Configuration > System Administration > Reboot**

The LoadMaster takes approximately 60 seconds to restart. During the restart time, all interfaces are down.

5.4 System Shutdown

To shut down the system:

a. In the left frame menu, click **System Configuration > System Administration > Shutdown**

Clicking this button attempts to power down the LoadMaster. If, for some reason, the power down fails, it will at a minimum halt the CPU.

5.5 Reset Machine

To reset the system to factory defaults:

a. In the left frame menu, click **System Configuration > System Administration > Reset Machine**

Reset the configuration of the appliance with exception of the license and username and password information. This only applies to the active appliance in a HA pair.

5.6 Start-up and Self-Test

The TSF shall run a suite of the following self-tests [during initial start-up (on power on)] to demonstrate the correct operation of the TSF:

- File systems checks

  During boot up the TSF checks file system by verifying the metadata and that it is mounted correctly
- SHA-256 Software integrity checks

  The TSF generates a SHA-256 has of the firmware image and compares it with the stored value
- Cryptographic algorithm known answer tests

  For each cryptographic algorithm, the TSF performs a sample cryptographic operation using know values and compares the output with the expected value
- Cryptographic algorithm pairwise constancy test

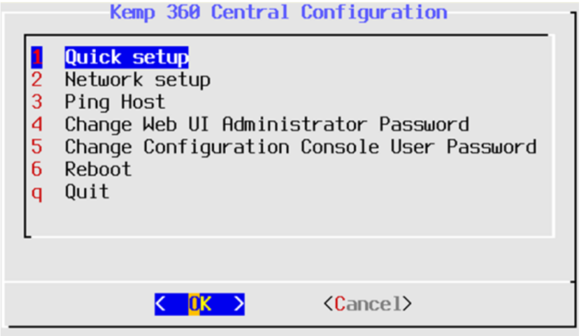
  For each cryptographic algorithm with a key-pair, the TSF performs a sample operation using know value and compares the output with the corresponding key-pair
- Health test of the noise source

  This is a continuous health-test that checks the number of occurrences of 6 different bit patterns in each 256-bit output from the noise source. It checks if any of the pattern counts are outside of predetermined thresholds. If more than 128 of the most recent 256 256-bit samples fails, the Entropy Source cease to output data

If any of these tests fail, the product halts or enters an error state. An administrator should contact Kemp Support in case of the TOE does not complete the boot sequence.

5.7 Logging Out

1. After a user has logged in, they may log out by clicking the Logout button, ⇥, in the top righthand corner of the screen if they have GUI (remote) access.
2. The console main menu appears whenever the console is accessed.

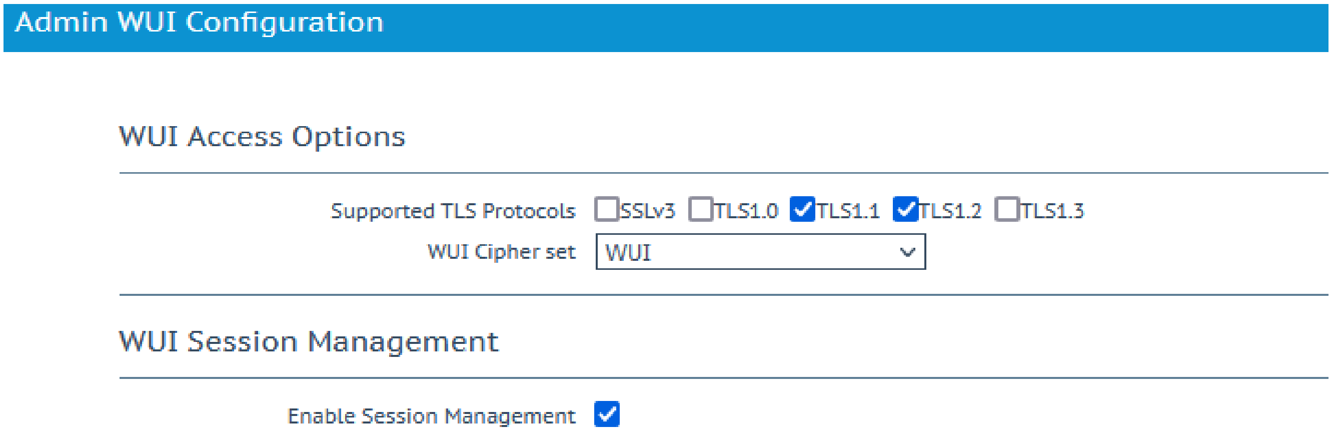


```
Kemp 360 Central Configuration

1  Quick setup
2  Network setup
3  Ping Host
4  Change Web UI Administrator Password
5  Change Configuration Console User Password
6  Reboot
q  Quit

        <  OK  >        <Cancel>
```

3. Press q to Quit the console session.

5.8 Admin WUI Access

Kemp LoadMaster supports versions 1.0, 1.1, 1.2 and 1.3 of the Transport Layer Security (TLS) protocol. In the evaluated configuration, the TLS1.1 and TLS1.2 should be used.



Admin WUI Configuration

WUI Access Options

Supported TLS Protocols ☐SSLv3 ☐TLS1.0 ☑TLS1.1 ☑TLS1.2 ☐TLS1.3

WUI Cipher set: WUI

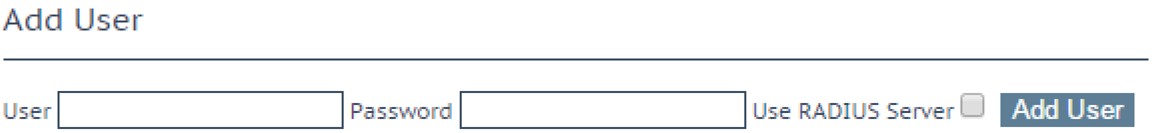
WUI Session Management

Enable Session Management ☑

a. In the left frame menu, click **Certificates & Security > Admin WUI Access > Select TLS1.1 and TLS1.2**

5.9 User Creation

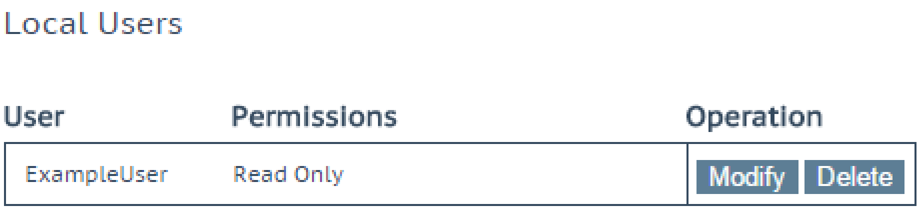
1. For Local Users creation navigate to **System Configuration** (in the left frame menu) **> System Administration > User Management > Add User**



Add User

User [ ] Password [ ] Use RADIUS Server ☐ Add User

2. Usernames can be a maximum of 64 characters long. Usernames can start with a digit and can contain alphanumeric characters, in addition to the following special characters: **=~^._+#@/-**
3. The minimum password length is defined by what is set in the Minimum password length field. All characters are allowed.
4. To modify or delete a Local User navigate to **System Configuration** (in the left frame menu) **> System Administration > User Management > Local User**



Local Users

User	Permissions	Operation
ExampleUser	Read Only	Modify Delete

5. The **Local Users** section lists any existing local users. Two options are available for existing users:
   - **Modify:** Change details for an existing local user, such as their permissions and password. For further information, refer to the Modify User section.
   - **Delete**: Delete the relevant user.

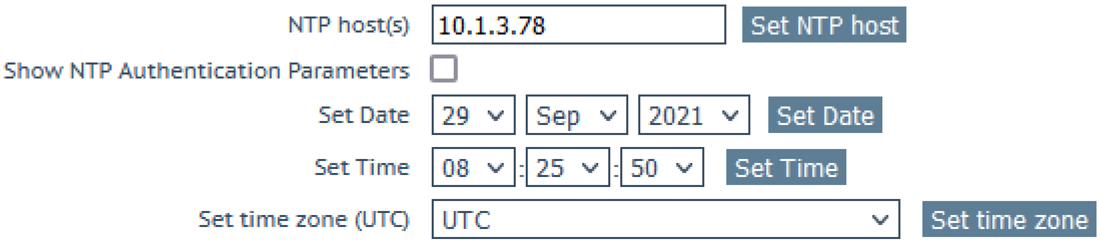
5.10 Zeroization

The keys stored in RAM are overwritten with zeros when session closes.
The keys stored in Restricted Filesystem access are zeroized by a Zeroize command.

5.11 Setting Date/Time

You can manually configure the date and time of LoadMaster.

1. In the left frame menu, click **System Configuration > System Administration > Date/Time:**
   a. **Set Date**: Set the date on the LoadMaster.
   b. **Set Time**: Set the time on the LoadMaster.
   c. **Set time zone**: Set the time zone where the LoadMaster is located.



NTP host(s) 10.1.3.78

Show NTP Authentication Parameters □

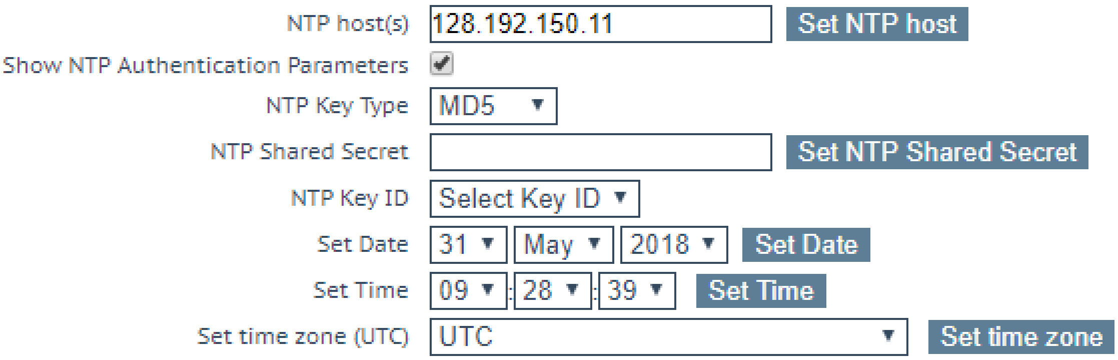
Set Date 29 Sep 2021

Set Time 08 : 25 : 50

Set time zone (UTC) UTC

5.12 Configuring NTP Server

You can manually configure the date and time of LoadMaster or leverage an NTP server. It supports time updates using NTPv4. The LoadMaster authentications updates using an administrator configured symmetric key and SHA-1. The TOE rejects broadcast and multicast time updates. The TOE allows up to 10 NTP time sources to be configured.



NTP host(s) 128.192.150.11

Show NTP Authentication Parameters ☑

NTP Key Type MD5

NTP Shared Secret

NTP Key ID Select Key ID

Set Date 31 May 2018

Set Time 09 : 28 : 39

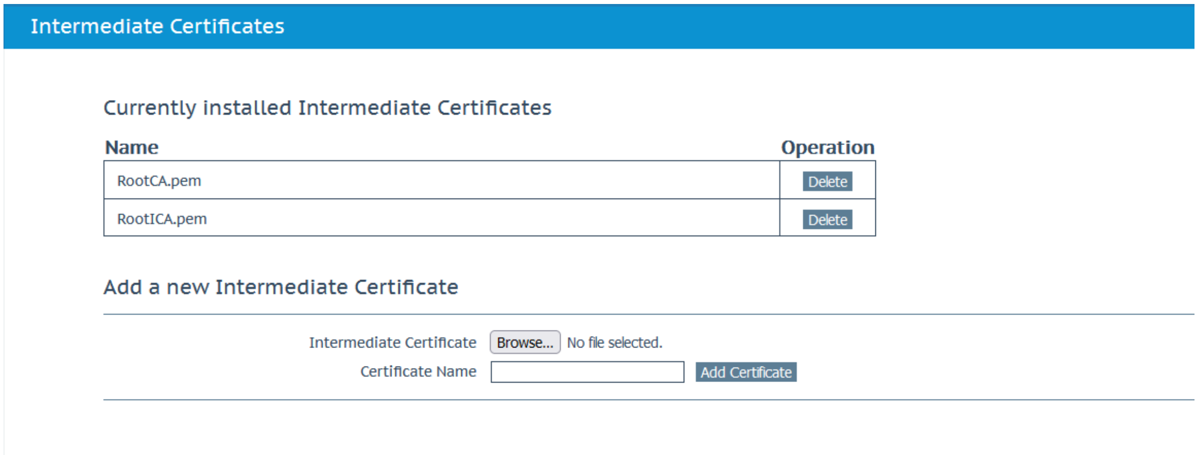
Set time zone (UTC) UTC

9. In the left frame menu, click **System Configuration > System Administration > Date/Time:**
   a. **NTP host(s)**: Specify the host which is to be used as the NTP server.
   b. **Show NTP Authentication Parameters**: Enable the Show NTP Authentication Parameters check box to display the parameters that are needed to support NTP authenticated requests. Disable the Show NTP Authentication Parameters checkbox to hide.
   c. **NTP Key Type**: Select either the MD5, SHA-1, or legacy SHA NTP key type. MD5 is the default value.
   d. **NTP Shared Secret**: The NTP shared secret string. The NTP secret can be a maximum of 20 ASCII characters long or 40 hexadecimal characters long.
   e. **NTP Key ID**: Select the NTP key ID. The values range from 1 to 99. Different key IDs can be used for different servers.
   f. **Set Date**: Set the date on the LoadMaster.
   g. **Set Time**: Set the time on the LoadMaster.
   h. **Set time zone**: Set the time zone where the LoadMaster is located.

5.13 Set the GUI Banner

1. In the left frame menu, click **Certificates & Security > Admin WUI Access**
2. Type in a **Pre-Auth Click Through Banner** and click **Set Pre-Auth Message**

5.14 Intermediate Certificate



Intermediate Certificates

Currently installed Intermediate Certificates

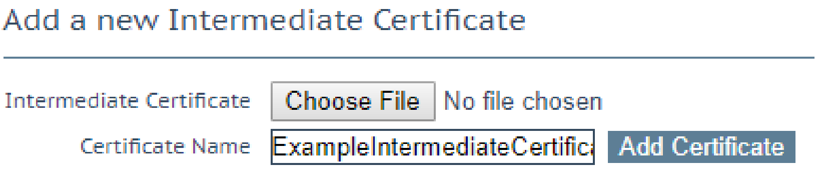
Name	Operation
RootCA.pem	Delete
RootICA.pem	Delete

Add a new Intermediate Certificate

Intermediate Certificate: Browse... No file selected.

Certificate Name: Add Certificate

This screen shows a list of the installed certificates and the name assigned to them. The **Intermediate Certificates** field allows you to assign intermediate and root certificates.



Add a new Intermediate Certificate

Intermediate Certificate: Choose File No file chosen

Certificate Name: ExampleIntermediateCertific Add Certificate

If you already have a certificate, or you have received one from a CSR, you can install the certificate by clicking the **Choose File** button. Navigate to and select the certificate and then enter the desired **Certificate Name**. The name can only contain alpha characters with a maximum of 32 characters.

Uploading several consecutive intermediate certificates within a single piece of text, as practiced by some certificate vendors such as GoDaddy, is allowed. The uploaded file is split into the individual certificates.

You can also delete the certificates by clicking the '**Delete'** button shown in the first screenshot of this section.

If a connection is not possible because the validity of a certificate cannot be determined, there is no override option. A valid certificate must be presented. This may include installing required certificates in the trust store i.e. uploading the certificates in **Intermediate Certificate** field.

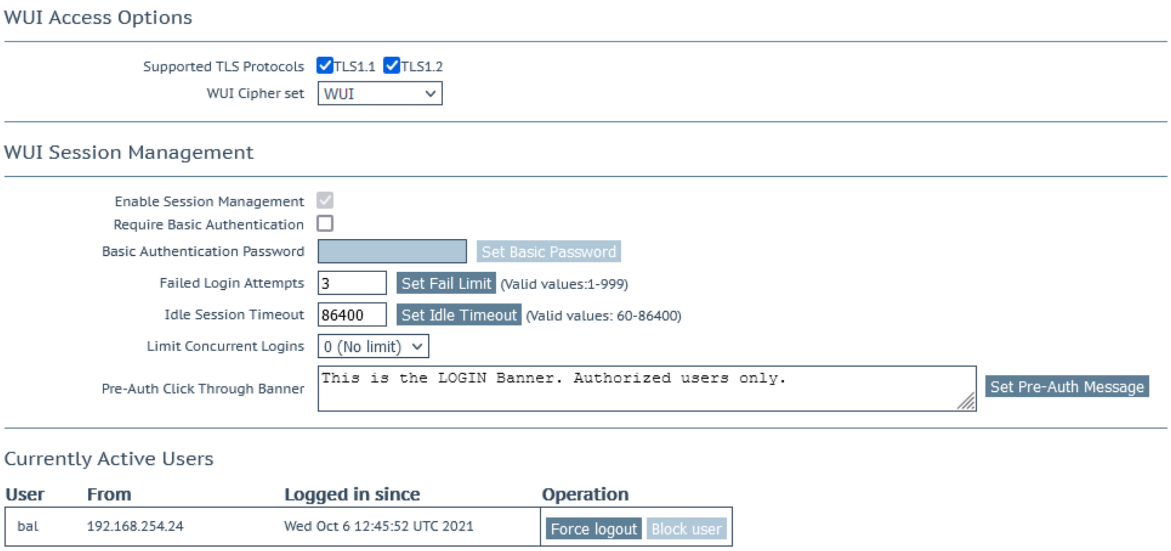
5.15 Set Admin UI for Login, TLS and Custom ECC Cipher Suite Set

1. In the left frame menu, click **Certificates & Security > Intermediate Certificates** and use the controls there to upload the issuing CA and associated Root CA certificate needed to validate admin client connections to the UI.
2. In the left frame menu, click **Certificates & Security > Admin WUI Access**:

a. In the **WUI Cipher Set** drop-down, select an appropriate Custom ECC Cipher Suite Set that has been generated. The Custom Cipher Suite Set can be generated from **Security & Certificates > Cipher Sets**

b. Enable/Disable **TLS Protocols** as required.

c. Set a Pre-Auth Click Through Banner (this is required for Certificate based authentication to the UI).



WUI Access Options

Supported TLS Protocols ☑TLS1.1 ☑TLS1.2
WUI Cipher set WUI

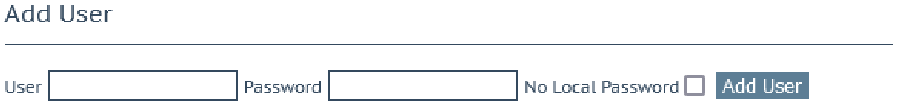
WUI Session Management

Enable Session Management ☑
Require Basic Authentication □
Basic Authentication Password
Failed Login Attempts 3 (Valid values:1-999)
Idle Session Timeout 86400 (Valid values: 60-86400)
Limit Concurrent Logins 0 (No limit)
Pre-Auth Click Through Banner This is the LOGIN Banner. Authorized users only.

Currently Active Users

User	From	Logged in since	Operation
bal	192.168.254.24	Wed Oct 6 12:45:52 UTC 2021	Force logout Block user

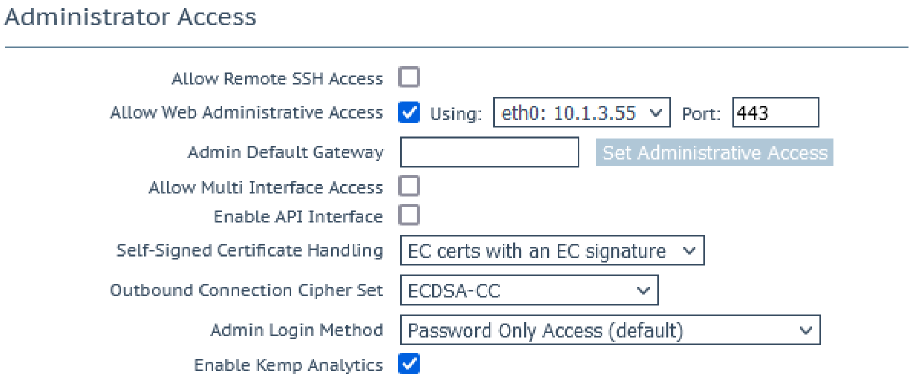
3. In the left frame menu, click **System Configuration > System Administration >User Management**
   a. Create a user account that exactly matches the Principal Name on the certificate you will use for administrative access (select the option to create the account without a password)
   b. Assign privileges to the account just created. Use "All Rights" for the first account added.



Add User

User Password No Local Password □

4. In the left frame menu, click **Certificates & Security > Remote Access**:
   a. Set the Admin Login field to **Password or Client Certificate**
   b. Test login using the associated certificate. If this fails, clear cookies, close browser, reopen browser and try again. If this still fails, clear cookies, close browser, reopen browser, bypass certificate request and sign in using the "bal" account.



Administrator Access

Allow Remote SSH Access ☐

Allow Web Administrative Access ☑ Using: eth0: 10.1.3.55 Port: 443

Admin Default Gateway [ ]

Allow Multi Interface Access ☐

Enable API Interface ☐

Self-Signed Certificate Handling: EC certs with an EC signature

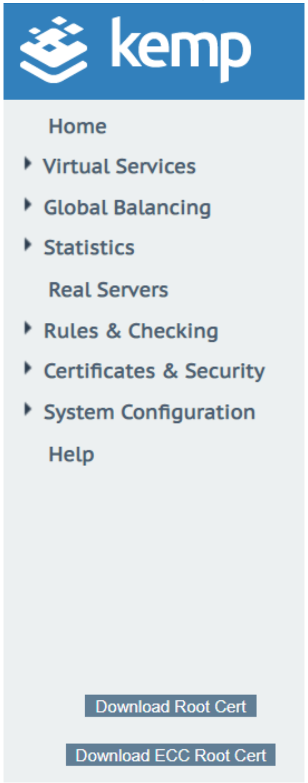
Outbound Connection Cipher Set: ECDSA-CC

Admin Login Method: Password Only Access (default)

Enable Kemp Analytics ☑

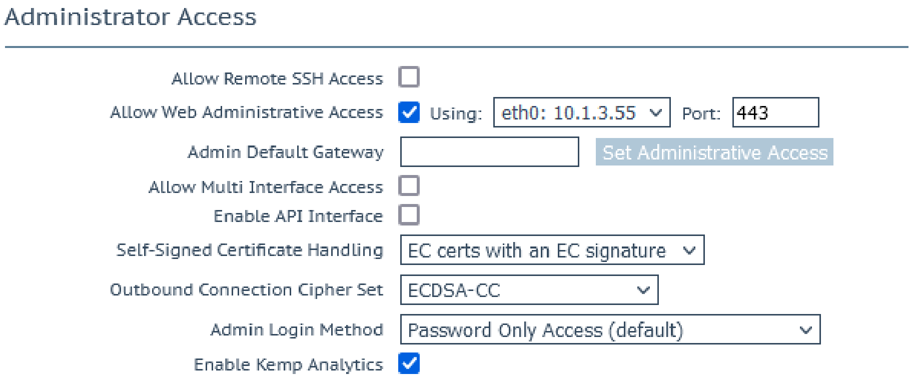
5.16 Set ECC Ciphers for Self-Signed Certificates and Outbound Connections

1. In the left frame menu, click **Certificates & Security > Remote Access**:
   a. In the **Self-Signed Certificate Handling** drop-down, select **EC Certs with an RSA signature**. This will autogenerate a new self-signed LoadMaster certificate and assign it to the WUI interface.
   b. Download the LoadMaster ECC Issuing CA Certificate and install in the management workstation certificate store and/or browser certificate store.



   c. In the **Self-Signed Certificate Handling** drop-down, select **EC Certs with an EC signature**. This will autogenerate a new self-signed LoadMaster certificate and assign it to the WUI interface. If you did not download and install the LoadMaster ECC issuing CA certificate, you will no longer be able to use the WUI. Use the console and perform a factory reset and start over. Factory reset does not change the "bal" password. [**Note**: When set to this value, all Certificate Signing Requests generated on the **Certificates & Security > Generate CSR** page will also use EC signatures.]

d. In the **Outbound Connection Cipher Set** drop-down, select an appropriate Custom ECC Cipher Suite Set. (Please see Appendix A for a list of the specific ciphers included in this cipher set and notes in relation to this item.)



Administrator Access

Allow Remote SSH Access	□
Allow Web Administrative Access	☑ Using: eth0: 10.1.3.55 Port: 443
Admin Default Gateway	Set Administrative Access
Allow Multi Interface Access	□
Enable API Interface	□
Self-Signed Certificate Handling	EC certs with an EC signature
Outbound Connection Cipher Set	ECDSA-CC
Admin Login Method	Password Only Access (default)
Enable Kemp Analytics	☑

5.17 Hash Cryptographic Operation (Hash Algorithm)

- The TOE supports cryptographic hashing services in accordance with a specified cryptographic algorithm SHA-1, SHA-256, SHA-384, SHA-512 and message digest sizes 160, 256, 384, 512 bits that meet the following: ISO/IEC 10118-3:2004.
- The TOE comes preconfigured for these sizes and no additional configuration is required.

5.18 Keyed Hash Cryptographic Operation (Keyed Hash Algorithm)

- The TOE supports keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and cryptographic key sizes 160-bits, 256-bits, 384-bits, and message digest sizes 160, 256, 384 bits that meet the following: ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”.
- The TOE comes preconfigured for these sizes and no additional configuration is required.

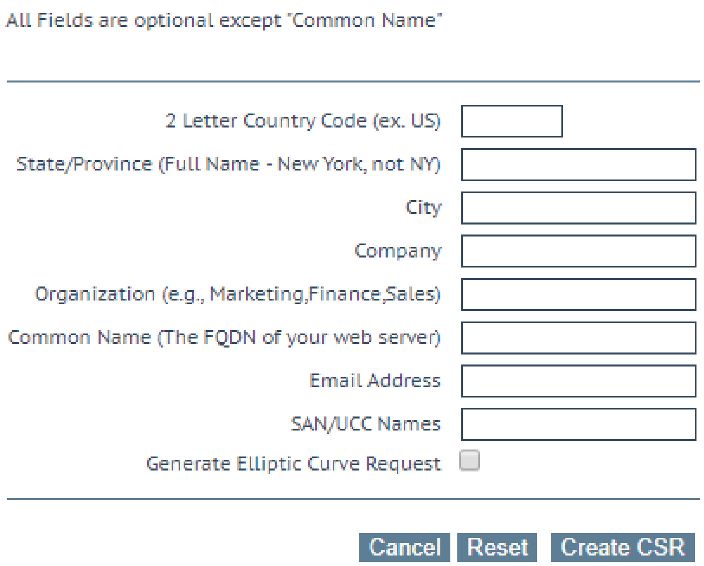
5.19 Random Bit Generation

- The TOE supports random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES).

5.20 Generate CSR (Certificate Signing Request)

- If you do not have a certificate, you may complete the Certificate Signing Request (CSR) form and click the **Create CSR** button. CSRs generated by the LoadMaster use SHA256.
- If **Self-Signed Certificate Handling** is set to **EC certs with an EC signature** (in **Certificates & Security > Remote Access**), CSR generation is restricted to the administrative (**bal**) user only. If **Self-Signed Certificate Handling** is set to a different value, all users (regardless of their permissions) can generate CSRs.

   1. In the main menu, go to **Certificates & Security > Generate CSR.**



All Fields are optional except "Common Name"

2 Letter Country Code (ex. US)	
State/Province (Full Name - New York, not NY)	
City	
Company	
Organization (e.g., Marketing,Finance,Sales)	
Common Name (The FQDN of your web server)	
Email Address	
SAN/UCC Names	
Generate Elliptic Curve Request	□

The following are the instructions for establishing the above fields in the CSR:

- **2 Letter Country Code (ex. US)**

The 2-letter country code that should be included in the certificate, for example **US** should be entered for the United States.

- **State/Province (Entire Name – New York, not NY)**

The state which should be included in the certificate. Enter the full name here, for example **New York**, not NY.

- **City**

The name of the city that should be included in the certificate.

- **Company (Organization)**

The name of the organization or company which should be included in the certificate.

- **Organization Unit (e.g., Marketing, Finance, Sales)**

The department or organizational unit that should be included in the certificate.

- **Common Name**

The Fully Qualified Domain Name (FQDN) for your web server.

- **Email Address**

The email address of the responsible person or organization that should be contacted regarding this certificate.

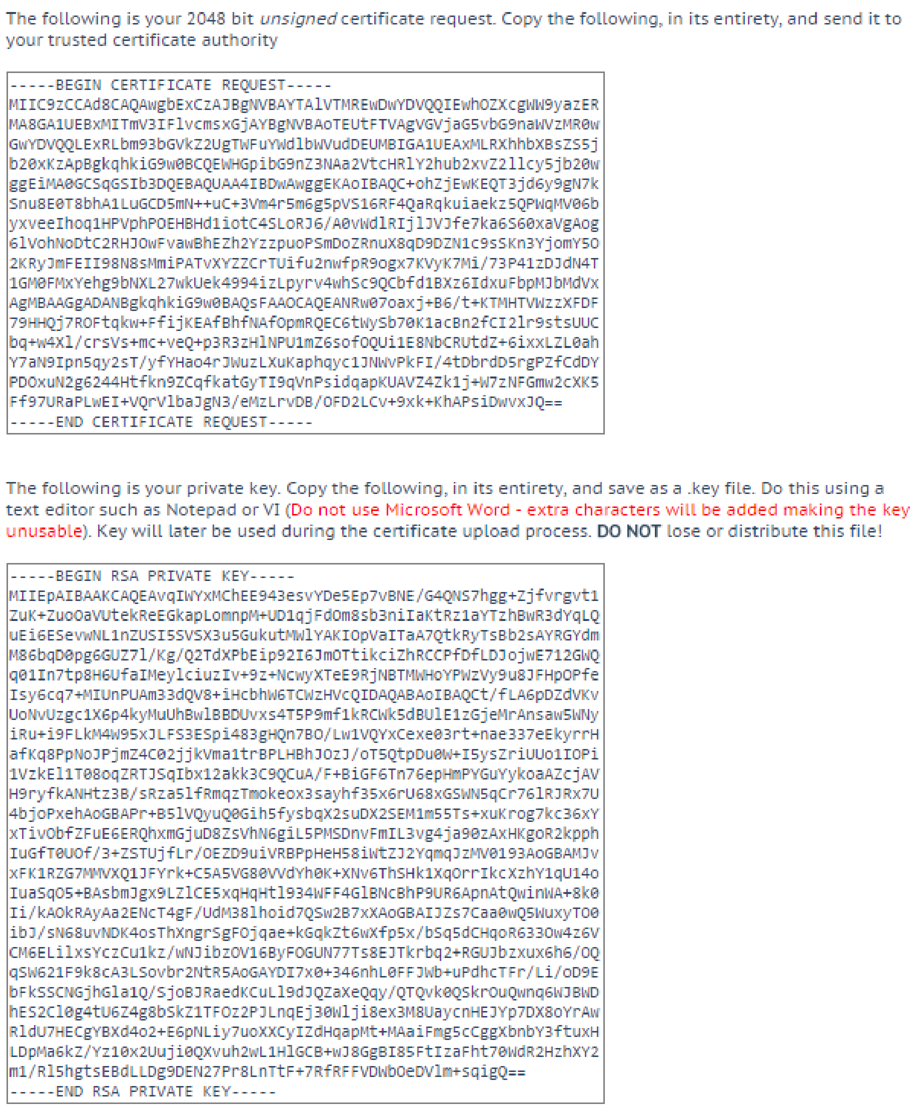
- **SAN/UCC Names**

A space-separated list of alternate names.

- **Generate Elliptical Curve Request**

Select this check box to generate an Elliptical Curve (EC) request instead of an RSA request.

2. Fill in the details in the resulting screen. The **Common Name** field is mandatory, all other fields are optional.
3. Click **Create CSR.**
4. Alter clicking the **Create CSR** button, the following screen appears:



The following is your 2048 bit *unsigned* certificate request. Copy the following, in its entirety, and send it to your trusted certificate authority

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC9zCCAd8CAQAwgbExCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhOZXcgWW9yazER
MA8GA1UEBxMITmV3IFlvcmsxGjAYBgNVBAoTEUtFTVAgVGVjaG5vbG9naWVzMR0w
GwYDVQQLExRLbm93bGVkZ2UgTWFuYWdlbWVudDEUMBIGA1UEAxMLRXhhbXBsZS5j
b20xKzApBgkqhkiG9w0BCQEWHGpibG9nZ3NAa2VtcHRlY2hub2xvZ2llcy5jb20w
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC+ohZjEwKEQT3jd6y9gN7k
Snu8E0T8bhA1LuGCD5mN++uC+3Vm4r5m6g5pVS16RF4QaRqkuiaekz5QPWqMV06b
yxveeIhoq1HPVphPOEHBHd1iotC4SLoRJ6/A0vWdlRIjlJVJfe7ka6S60xaVgAog
6lVohNoDtC2RHJOwFvawBhEZh2YzzpuoPSmDoZRnuX8qD9DZN1c9sSKn3YjomY5O
2KRyJmFEII98N8sMmiPATvXYZZCrTUifu2nwfpR9ogx7KVyK7Mi/73P41zDJdN4T
1GM0FMxYehg9bNXL27wkUek4994izLpyrv4whSc9QCbfd1BXz6IdxuFbpMJbMdVx
AgMBAAGgADANBgkqhkiG9w0BAQsFAAOCAQEANRw07oaxj+B6/t+KTMHTVWzzXFDF
79HHQj7ROFtqkw+FfijKEAfBhfNAfOpmRQEC6tWySb70K1acBn2fCI2lr9stsUUC
bq+w4Xl/crsVs+mc+veQ+p3R3zHlNPU1mZ6sofOQUi1E8NbCRUtdZ+6ixxLZL0ah
Y7aN9Ipn5qy2sT/yfYHao4rJWuzLXuKaphqyc1JNWvPkFI/4tDbrdD5rgPZfCdDY
PDOxuN2g6244Htfkn9ZCqfkatGyTI9qVnPsidqapKUAVZ4Zk1j+W7zNFGmw2cXK5
Ff97URaPLwEI+VQrVlbaJgN3/eMzLrvDB/OFD2LCv+9xk+KhAPsiDwvxJQ==
-----END CERTIFICATE REQUEST-----
```

The following is your private key. Copy the following, in its entirety, and save as a .key file. Do this using a text editor such as Notepad or VI (Do not use Microsoft Word - extra characters will be added making the key unusable). Key will later be used during the certificate upload process. **DO NOT** lose or distribute this file!

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAvqIWYxMChEE943esvYDe5Ep7vBNE/G4QNS7hgg+Zjfvrgvt1
ZuK+ZuoOaVUtekReEGkapLomnpM+UD1qjFdOm8sb3niIaKtRz1aYTzhBwR3dYqLQ
uEi6ESevwNL1nZUSI5SVSX3u5GukutMWlYAKIOpVaITaA7QtkRyTsBb2sAYRGYdm
M86bqD0pg6GUZ7l/Kg/Q2TdXPbEip92I6JmOTtikciZhRCCPfDfLDJojwE712GWQ
q01In7tp8H6UfaIMeylciuzIv+9z+NcwyXTeE9RjNBTMWHoYPWzVy9u8JFHpOPfe
Isy6cq7+MIUnPUAm33dQV8+iHcbhW6TCWzHVcQIDAQABAoIBAQCt/fLA6pDZdVKv
UoNvUzgc1X6p4kyMuUhBwlBBDUvxs4T5P9mf1kRCWk5dBUlE1zGjeMrAnsaw5WNy
iRu+i9FLkM4W95xJLFS3ESpi483gHQn7BO/Lw1VQYxCexe03rt+nae337eEkyrrH
afKq8PpNoJPjmZ4C02jjkVma1trBPLHBhJOzJ/oT5QtpDu0W+I5ysZriUUo1IOPi
1VzkEl1T08oqZRTJSqIbx12akk3C9QCuA/F+BiGF6Tn76epHmPYGuYykoaAZcjAV
H9ryfkANHtz3B/sRza5lfRmqzTmokeox3sayhf35x6rU68xGSWN5qCr76lRJRx7U
4bjoPxehAoGBAPr+B5lVQyuQ0Gih5fysbqX2suDX2SEM1m55Ts+xuKrog7kc36xY
xTivObfZFuE6ERQhxmGjuD8ZsVhN6giL5PMSDnvFmIL3vg4ja90zAxHKgoR2kpph
IuGfT0UOf/3+ZSTUjfLr/OEZD9uiVRBPpHeH58iWtZJ2YqmqJzMV0193AoGBAMJv
xFK1RZG7MMVXQ1JFYrk+C5A5VG80VVdYh0K+XNv6ThSHk1XqOrrIkcXzhY1qU14o
IuaSqO5+BAsbmJgx9LZlCE5xqHqHtl934WFF4GlBNcBhP9UR6ApnAtQwinWA+8k0
Ii/kAOkRAyAa2ENcT4gF/UdM38lhoid7QSw2B7xXAoGBAIJZs7Caa0wQ5WuxyTO0
ibJ/sN68uvNDK4osThXngrSgFOjqae+kGqkZt6wXfp5x/bSq5dCHqoR633Ow4z6V
CM6ELilxsYczCu1kz/wNJibzOV16ByFOGUN77Ts8EJTkrbq2+RGUJbzxux6h6/OQ
qSW621F9k8cA3LSovbr2NtR5AoGAYDI7x0+346nhL0FFJWb+uPdhcTFr/Li/oD9E
bFkSSCNGjhGla1Q/SjoBJRaedKCuLl9dJQZaXeQqy/QTQvk0QSkrOuQwnq6WJBWD
hES2Cl0g4tU6Z4g8bSkZ1TFOz2PJLnqEj30Wlji8ex3M8UaycnHEJYp7DX8oYrAw
RldU7HECgYBXd4o2+E6pNLiy7uoXXCyIZdHqapMt+MAaiFmg5cCggXbnbY3ftuxH
LDpMa6kZ/Yz10x2Uuji0QXvuh2wL1HlGCB+wJ8GgBI85FtIzaFht70WdR2HzhXY2
m1/Rl5hgtsEBdLLDg9DEN27Pr8LnTtF+7RfRFFVDWbOeDVlm+sqigQ==
-----END RSA PRIVATE KEY-----
```

5. The top part of the screen should be copied and pasted into a plain text file and sent to the Certificate Authority of your choice. They will validate the information and return a validated certificate.
6. The lower part of the screen is your private key and should be kept in a safe place. This key should not be disseminated as you will need it to use the certificate. Copy and paste the private key into a plain text file (do not use an application such as Microsoft Word) and keep the file safe.
7. The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

5.21 Auditing

Kemp LoadMaster sends audit records to the external server as the audit records are generated. It transmits generated audit data to an external server using the TLS trusted channel. It does not retransmit audit logs that were generated while the connection to the audit server was down.

When local audit storage is exhausted, the TSF will not record new events locally until additional space is available. Records are still transmitted to the external server, and so the audit trail is preserved. Local audit records will be temporarily stored in a buffer until they can be stored. The TSF allows all available space to be used to store audit records. For the Virtual Load Master that is up to 7GB. The HW Load Master models have up to 25GB of space available to store audit records.

The Kemp LoadMaster generates a warning log when audit storage reaches 85% of capacity to inform the administrator that audit storage is nearing capacity.

The **Disk Usage** under **System Configuration > System Administration > System Log Files** provides a visual indication of the percentage used/free of the log partition. Color-coding is used to highlight different usage levels:

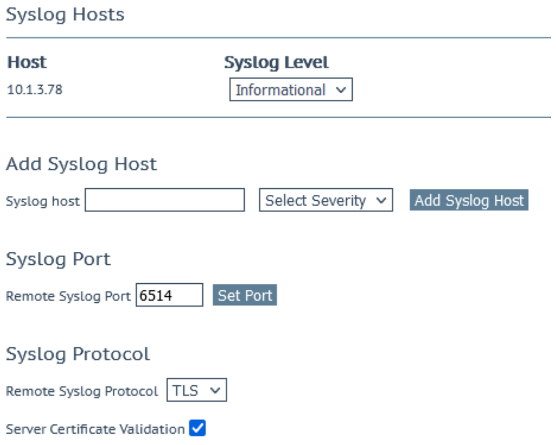
- 0% to 50%: green
- 50% to 90%: orange
- 90% to 100%: red

The TSF prevents unauthorized users from modifying or deleting audit records.

5.22 Secure Remote Logging

The LoadMaster can produce various warning and error messages using the syslog protocol. Syslog messages comply with RFC5424. These messages are normally stored locally. Syslog messages are transmitted securely using TLS to remote servers. The LoadMaster uses OCSP to check the validity of the server certificates supplied by configured syslog servers. If these checks fail, connections to the server are not permitted.

1. In the left frame menu, click **System Configuration > System Log Files > Syslog Options**
2. By entering the relevant IP address in the **Syslog host** text box and select the severity and click **Add Syslog Host**
3. Also enter the **Syslog Port** enter *any port other than 601* and click on **Set Port**.
4. Select the **Syslog Protocol** either TCP,UDP or TLS.
5. Enable the Server Certificate Validation
    a. Note: secure syslog channel is restricted to TLSv1.1 and TLSv1.2



Syslog Hosts

Host	Syslog Level
10.1.3.78	Informational

Add Syslog Host

Syslog host [ ] Select Severity Add Syslog Host

Syslog Port

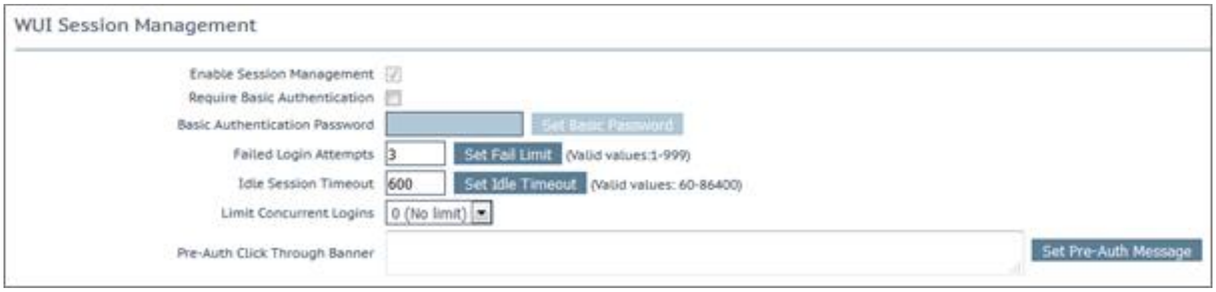
Remote Syslog Port 6514 Set Port

Syslog Protocol

Remote Syslog Protocol TLS

Server Certificate Validation ☑

5.23 Failed Login Attempts



WUI Session Management

Enable Session Management ☑
Require Basic Authentication □
Basic Authentication Password
Failed Login Attempts 3 (Valid values:1-999)
Idle Session Timeout 600 (Valid values: 60-86400)
Limit Concurrent Logins 0 (No limit)
Pre-Auth Click Through Banner

1. In the left frame menu, click **System Configuration > Certificate & Security > Admin WUI Access > Failed Login Attempts:** Set the Failed Login Attempts number.
2. The number of times that a user can fail to login correctly before they are blocked can be specified within this text box. The valid values that may be entered are numbers between **1** and **999**.
3. If a user is blocked, only the **bal** user or other users with **All Permissions** set can unblock a blocked user.
4. If the **bal** user is blocked, there is a 'cool-down' period of ten minutes before the bal user can login again.

5.24 Idle Session Timeout

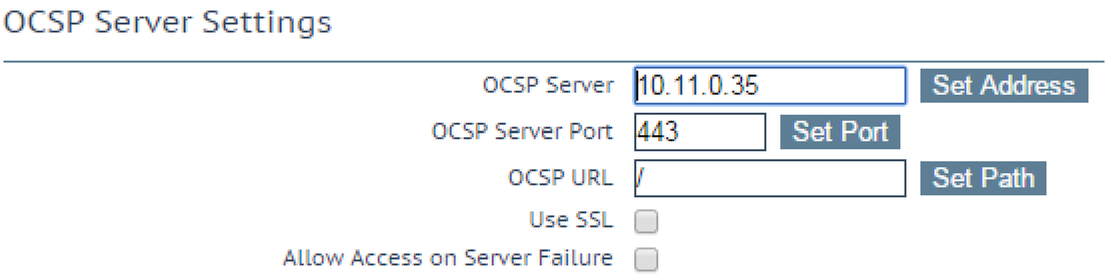
1. In the left frame menu, click **System Configuration > Certificate & Security > Admin WUI Access > Idle Session Timeout:** The length of time (in seconds) a user can be idle (no activity recorded) before they are logged out of the session.
2. The valid values that may be entered are numbers between **60** and **86400** (between one minute and 24 hours).

5.25 Disable SSH Access

1. In the left frame menu, click **Certificates & Security > Remote Access**, and disable the **Allow Remote SSH Access** check box.

5.26 Enable OCSP Checking

1. In the left frame menu, click **Certificates & Security > OCSP Configuration**:
   a. Enter the **OCSP Server** IP address and click **Set Address**.
   b. Enter the **OCSP Server Port** and click **Set Port**.
   c. Enter the **OCSP URL** and click **Set URL**.
   d. Enable the **Enable OCSP Checking** check box.



OCSP Server Settings

OCSP Server: 10.11.0.35 Set Address

OCSP Server Port: 443 Set Port

OCSP URL: / Set Path

Use SSL □

Allow Access on Server Failure □

   e. If the certificate cannot be validated because the server is unavailable, there is an option called **Allow Access on Server Failure** where you can decide if you want to pass the authentication or not. Enabling this check box treats an OCSP server connection failure or timeout as if the OCSP server has returned a valid response. That is, the client certificate is treated as valid.

Note: The AIA is given precedence and will be used based on its presence. If the AIA is not present or appears invalid, the **OCSP Server** configuration details will be used.
Please note the following:
- LDAPS: AIA information from the server certificate is honoured if **Certificates & Security > OCSP Configuration > OCSP Checking** is enabled.
- Syslog-NG: AIA information from the server certificate is honoured if **Certificates & Security > OCSP Configuration > OCSP Checking** is enabled.
- WUI Authentication: AIA information from the client certificate is honoured if the "Client certificate required (verify via OCSP)" is configured under **Certificates & Security > Remote Access > Administrator Access > Admin Login Method.**

5.27 SAN Extensions

- The TOE supports the reference identifier per RFC 6125 section 6, IPv4 address in CN or SAN, IPv4 address in SAN.
- The TOE only checks the identifier in the CN if the SAN extension is not present. The TSF does not support SRV or URI identifiers.
- The TLS client will transmit the Supported Elliptic Curves extension in the Client Hello message by default with support for the following NIST curves: secp256r1, secp384r1, and secp521r1..
- The TSF then parses the SAN (when present) or Common Name from the certificate. The TSF the matches the identifier against a list of defined users or by sending the identifier to an LDAP server.

5.28 Reference Identifiers

- The reference identifier for external IT entities is configured by the administrator using the available administrative commands in the CLI. The reference identifiers must be an IPv4 address, or a hostname.

- When the reference identifier is a hostname, the TOE compares the hostname against all the DNS Name entries in the Subject Alternative Name (SAN) extension. If the hostname does not match any of the DNS Name entries, then the verification fails. If the certificate does not contain any DNS Name entries in SAN, the TOE will compare the hostname against the Common Name (CN). If the hostname does not match the CN, then the verification fails. For both DNS Name and CN matching, the hostname must be an exact match or wildcard match. In the case of a wildcard match, the wildcard must be the left-most component, wildcard matches a single component, and there are at least two non-wildcard components.
- When the reference identifier is an IP address, the TOE converts the IP address to a binary representation in network byte order. IPv4 addresses are converted directly from decimal to binary with period "." serving as the delineator. The TOE compares the binary IP address against all the IP Address entries in the Subject Alternative Name extension. If there is not an exact binary match, then the verification fails. If the SAN entry is missing, the TOE will compare the IPv4 address against the Common Name (CN). If the IPv4 address in CN is not an exact binary match, then the verification fails. For IPv4 address in SAN or CN matching, the IPv4 address must be an exact binary match.
  Note: SAN is prioritized over CN.
  Warning: The above-mentioned reference identifier matching rules should be taken into consideration while connecting to peers or IT entities using certificates that have DNS or IP Address.
- The TLS channel is terminated if verification fails.
- The TOE does not enforce canonical format.

5.29 Using CLI

The Command Line Interface allows users to interface with the LoadMaster via a command line shell or a menu-based series of options.

1. You will need a PC to connect via COM+ (Console) port with a terminal emulation application, or a standard VGA and keyboard. Use a null modem cable (reversal) to connect the COM+ port to the LoadMaster COM port on the rear of the unit.
2. The COM+ settings should be 115200, 8, N,1.
3. After initially deploying and powering on a LoadMaster, ideally the IP address of the LoadMaster will be obtained via DHCP.
4. If the IP address has not been obtained via DHCP, or if the address details of the LoadMaster need to be changed, the console can be used to configure the IP address of the LoadMaster, the default gateway address and the name server addresses.
5. To go through this menu, simply log in to the console using the default username and password **(bal and 1fourall)**.

5.30 Set the CLI Banner

1. In the left frame menu, click **Certificates & Security > Remote Access**.
2. Check the **Allow Remote SSH Access box**, type in an **SSH Pre-Auth Banner** and click **Set Pre-Auth Message**. This banner is also used for the CLI (even if SSH is disabled).

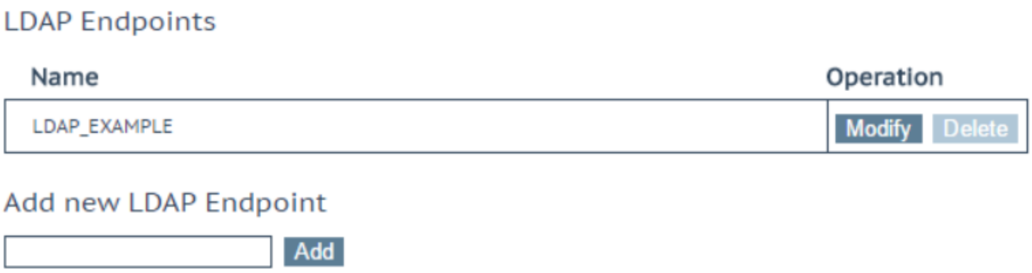
5.31 Disable CLI Virtual Service Administration

1. To disable CLI VS administration (to meet logging requirements):
   c. In the left frame menu, click **System Configuration > Logging Options > System Logs** and then do the following:
   d. In the page at right, click the **Debug Options** button.

e. Click **Disable CLI VS** Management. [Note that the button and label now read: Enable CLI VS Management.]

5.32 Setup Admin UI Access via LDAP

1. To set up an LDAP domain, click **Certificates & Security > LDAP Configuration**.



LDAP Endpoints

Name	Operation
LDAP_EXAMPLE	Modify Delete

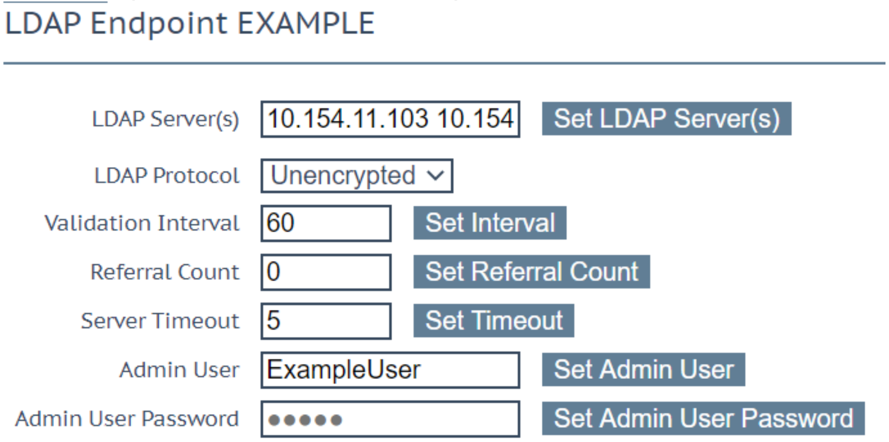
Add new LDAP Endpoint

This screen provides a management interface for LDAP endpoints. These LDAP endpoints may be used in three different areas:

- Health checks
- SSO domains
- WUI authentication

Any existing **LDAP Endpoints** are listed here, with an option to **Modify** and **Delete**. If an LDAP endpoint is in use, it cannot be deleted.

There is also an option to add a new LDAP endpoint. Type a name for the endpoint and click **Add**. Spaces and special characters are not permitted in the LDAP endpoint name.



LDAP Endpoint EXAMPLE

LDAP Server(s)	10.154.11.103 10.154
LDAP Protocol	Unencrypted
Validation Interval	60
Referral Count	0
Server Timeout	5
Admin User	ExampleUser
Admin User Password	●●●●●

- **LDAP Server(s)**

Specify a space-separated list of LDAP servers to be used. Port numbers can also be specified if required. If you have multiple domains and are using **Permitted Groups**, sometimes it is necessary to include the Global Catalog port number, otherwise the **Permitted Groups** will fail. The default port is **3628**. For example, **10.110.20.23:3268**.

The LoadMaster uses OCSP to check the validity of the server certificates supplied by configured LDAPS servers. If these checks fail, connections to the server are not permitted.

- **LDAP Protocol**

Select the transport protocol to use when communicating with the LDAP server.

If you create an SSO domain with the **Authentication Protocol** set to **Certificates**, ensure to set the **LDAP Protocol** to **LDAPS** in the LDAP endpoint.

- **Validation Interval**

Specify how often you should revalidate the user with the LDAP server.

- **Referral Count**

The LoadMaster offers beta functionality to support LDAP referral replies from Active Directory Domain Controllers. If this is set to **0**, referral support is not enabled. Set this field to a value between **1** and **10** to enable referral chasing. The number specified will limit the number of hops (referrals chased).

- **Server Timeout**

Specify the LDAP server timeout in seconds. The default value is **5**. Valid values range from **5** to **60**.

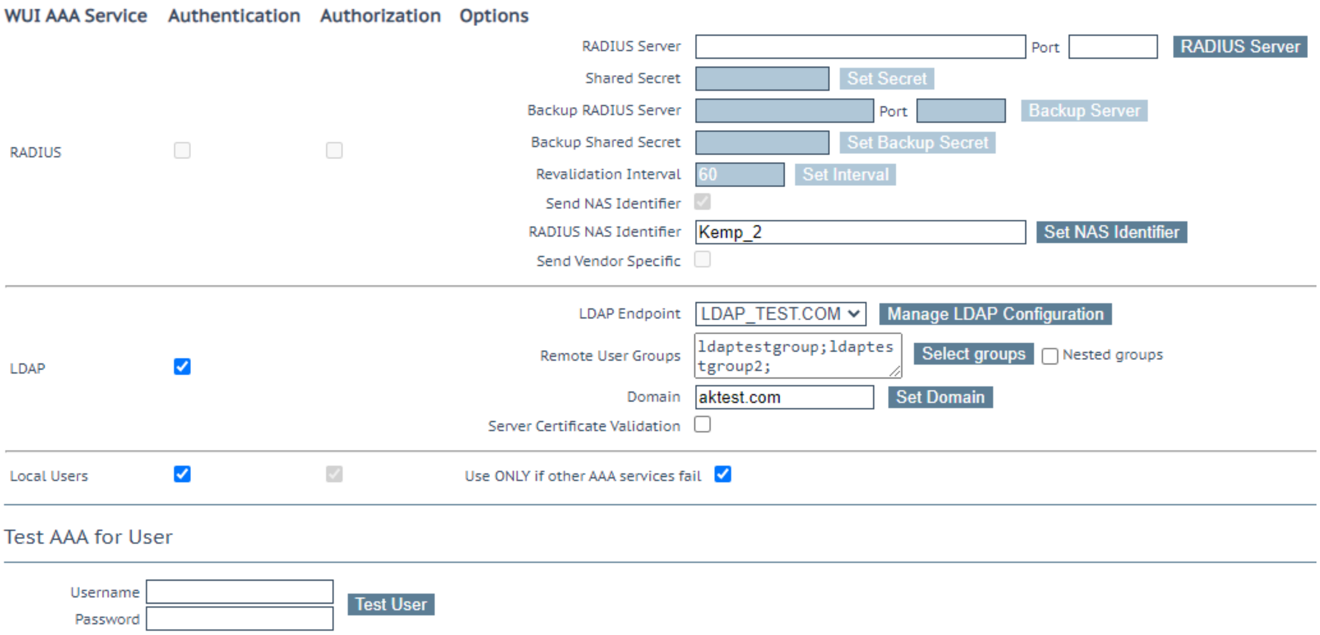
- **Admin User**

Type the username of an administrator user.

- **Admin User Password**

Type the password for the specified administrator user.

2. To set up admin UI (bal account) access via LDAP/AD:
   a. In the left frame menu, click **Certificates & Security > Remote Access**.
   b. In the page at right, click the **WUI Authorizations** button.



WUI AAA Service	Authentication	Authorization	Options
RADIUS	□	□	RADIUS Server: Port: Shared Secret Backup RADIUS Server: Port: Backup Shared Secret Revalidation Interval: 60 Send NAS Identifier ☑ RADIUS NAS Identifier: Kemp_2 Send Vendor Specific □
LDAP	☑		LDAP Endpoint: LDAP_TEST.COM Remote User Groups: ldaptestgroup;ldaptestgroup2; □ Nested groups Domain: aktest.com Server Certificate Validation □
Local Users	☑	☑	Use ONLY if other AAA services fail ☑

Test AAA for User

Username
Password

   c. Select the **LDAP** option.
   d. Select the **LDAP Endpoint** that is created.
   e. Add **Remote User Groups** if created.
   f. Add the **Domain** and enable **Server Certificate Validation** option.

Note: LDAPS channel is restricted to TLSv1.1 and TLSv1.2

5.33 Lockdown Admin UI logon to Certificate Only with OCSP validation

1. In the left frame menu, click **Certificates & Security > Remote Access**
    a. Set the Admin Login field to **Client Certificate Required (Verify via OCSP)**
    b. Sign out, clear cookies in management workstation browser, close browser, reopen browser and verify certificate logon works
    c. If login fails, you will need to use the Console interface to reset the web administrative settings to allow you to sign in using a password.

5.34 Logging for Admin UI logon

1. In the left frame menu, click **System Configuration -> Network Options**
    a. Set the **Log SSL errors** to **"All errors"**

5.35 Elliptical Curve Cipher Set

A Custom ECC Cipher Suite set can be configured with the claimed cipher suites. Currently the ST claims:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

The Custom ECC Cipher Suite set can be configured under **Certificates & Security > Cipher Sets.**

5.36 Installing an Update Image

To install an update image on LoadMaster:

1. Unzip the archive received from Kemp on a laptop or other device with a browser.
    - In it are the update image and an XML file.
2. Open the LoadMaster UI and navigate to **System Configuration > System Administration > Update Software**.
3. Click on the **Browse** button next to **Software Update File** and select the update image from Step 1.
4. Click on the **Browse** button next to **Verification File** and select the XML file from Step 1.
5. Click **Update Machine**. After the system validates the image, you'll be asked to confirm the installation to continue.
6. Once the update is completed, the system asks you to confirm rebooting the system.
7. On the **Home** page of the TOE the current version is seen.

Once the system reboots and the UI become active again, you can log in. Software image files are digitally signed so their integrity can be automatically verified during the upgrade process. An image that fails an integrity check will not be loaded.

The TOE gives error i.e., rejects software updates when one tries to update software with invalid software or without a signature xml file or with a different signature xml file. Audit log is generated when we try to update with invalid software or with a different signature xml file. The TOE does not support published hash used to protect the trusted update mechanism.

5.37 Sample Audit Logs

The following events generate audit logs:

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
FAU_GEN.1	• Start-up and shut-down of the audit functions. • Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators). • Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed). • Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged). • Resetting passwords (name	None.	• **Start-up and shut-down of the audit functions.** **Start-up of the audit functions:** 2022-12-16T14:38:11+00:00 lb100-X15 syslog-ng: syslog-ng starting up; version='3.25.1' 2022-12-16T14:38:12+00:00 lb100-X15 syslog-ng: System log started **Shut-down of the audit functions:** 2022-12-16T14:38:11+00:00 lb100-X15 syslog-ng: syslog-ng shutting down; version='3.25.1' • **Administrative login and logout (name of user account shall be logged if individual user accounts are required for Administrators).** **Administrative login:** 2021-02-22T09:11:31+00:00 lb100-X15 logger: User bal (10.1.1.66) Logged in (Session: vM0jXIta2kseJrlIhORB0xwz) **Administrative logout:** 2021-02-22T09:19:34+00:00 lb100-X15 logger: User bal (10.1.1.66) Logged out (Session: vM0jXIta2kseJrlIhORB0xwz) • **Changes to TSF data related to configuration changes (in addition to the information that a change occurred it shall be logged what has been changed).** **Configuration of new time server:**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
	of related user account shall be logged).		2021-04-07T07:51:12+00:00 lb100-X15 logger: User acumensec (192.168.254.143) set 'NTP_HOST' to '10.1.3.78' **Addition of the certificate to the TOE's Trust store:** 2021-04-07T08:04:51+00:00 lb100-X15 logger: User acumensec (192.168.254.143) Installed an Intermediate Certificate PD-IntermediateCA **Deleting of the certificate from the TOE's Trust store:** 2021-01-27T12:03:41+00:00 lb100-X15 logger: User acumensec (192.168.254.143) Deleted Intermedidate Certificate PD-IntermediateCA • **Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged).** 2021-02-23T05:35:46+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Logged in (Session: vnfG6vvRYXUisocsmnuH6VUz) 2021-02-23T05:38:00+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Generated a new Self Signed Admin Cert 2021-02-23T05:38:00+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Generated self signed certificate key for 10.1.3.55 • **Resetting passwords (name of related user account shall be logged).** 2023-01-04T11:40:29+00:00 lb100-X15 logger: User bal (192.168.228.155) Set password for user acumensec
FAU_GEN.2	None.	None.	NA
FAU_STG_EXT.1	None.	None.	NA
FAU_STG_EXT.3/LocSpace	Low storage space for audit events.	None.	2021-03-17T13:47:01+00:00 lb100-X15 logger: /var/log partition usage exceeded 93%

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
FCS_CKM.1	None.	None.	NA
FCS_CKM.2	None.	None.	NA
FCS_CKM.4	None.	None.	NA
FCS_COP.1/DataEncryption	None.	None.	NA
FCS_COP.1/SigGen	None.	None.	NA
FCS_COP.1/Hash	None.	None.	NA
FCS_COP.1/KeyedHash	None.	None.	NA
FCS_RBG_EXT.1	None.	None.	NA
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure	**Failure to establish connection through GUI:** 2021-02-19T09:41:33+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Login failed - Invalid user/password
FCS_NTP_EXT.1	• Configuration of a new time server • Removal of configured time server	Identity if new/removed time server	**Configuration of new time server:** 2021-04-07T07:51:12+00:00 lb100-X15 logger: User acumensec (192.168.254.143) set 'NTP_HOST' to '10.1.3.78' **Removal of Time server:** 2021-04-07T07:52:51+00:00 lb100-X15 logger: User acumensec (192.168.254.143) set 'NTP_HOST' to ''
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Reason for failure	2021-01-11T06:50:24+00:00 lb100-X15 validuser: do_ldap_check: ldap_sasl_bind_s(): rc=-1, bind failed for user [acumensec], error: error:14090086:SSL routines:ssl3_get_server_certificate:certificate verify failed (unsupported certificate purpose)
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	2021-02-01T13:22:02+00:00 lb100-X15 sslproxy: Client 10.1.1.66 failed SSL negotiation (ssl/statem/statem_srvr.c/2253): error:1417A0C1:SSL routines:tls_post_process_client_hello:no shared cipher)
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	2021-02-19T09:44:12+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Denied access - too many failed attempts
FIA_PMG_EXT.1	None.	None.	NA
FIA_UIA_EXT.1	All use of identification and	Origin of the attempt (e.g., IP address).	**Local connection with incorrect credentials:** 2021-02-22T06:38:34+00:00 lb100-X15 login: pam_unix(login:auth): authentication failure;

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
	authentication mechanism.		logname=LOGIN uid=0 euid=0 tty=/dev/ttyS0 ruser= rhost= user=bal 2021-02-22T06:38:37+00:00 lb100-X15 login: FAILED LOGIN (1) on '/dev/ttyS0' FOR 'bal', Authentication failure **Local connection with correct credentials:** 2021-02-22T06:47:34+00:00 lb100-X15 login: pam_unix(login:session): session opened for user bal by LOGIN(uid=0) **Remote connection with incorrect credentials:** 2021-02-22T06:51:47+00:00 lb100-X15 logger: User bal (10.1.1.66) Login failed - Invalid user/password **Remote connection with correct credentials:** 2021-02-22T06:53:49+00:00 lb100-X15 logger: User bal (10.1.1.66) Logged in (Session: DWAcx7GmQvhDAtXDUdC1cvcz)
FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).	2021-02-22T06:47:34+00:00 lb100-X15 login: pam_unix(login:session): session opened for user acumensec by LOGIN(uid=0) 2021-02-22T06:53:49+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Logged in (Session: DWAcx7GmQvhDAtXDUdC1cvcz)
FIA_UAU.7	None.	None.	NA
FIA_X509_EXT.1/Rev	- Unsuccessful attempt to validate a certificate - Any addition, replacement or removal of trust anchors in the TOE's trust store	- Reason for failure of certificate validation - Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	**Unsuccessful attempt to Validate Certificate:** 2021-01-27T12:06:39+00:00 lb100-X15 syslog-ng: Certificate validation failed; subject='C=US, OU=CC, O=Acumen, CN=10.1.3.78', issuer='CN=PD-IntermediateCA.acumensec.local, OU=CC, O=Acumen, C=US', error='unable to get local issuer certificate', depth='0' 2021-01-27T12:06:39+00:00 lb100-X15 syslog-ng: SSL error while writing stream; tls_error='SSL routines:ssl3_get_server_certificate:certificate verify failed' **Addition of the certificate to the TOE's Trust store:**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
			2021-04-07T08:04:51+00:00 lb100-X15 logger: User acumensec (192.168.254.143) Installed an Intermediate Certificate PD-IntermediateCA **Deleting of the certificate from the TOE's Trust store:** 2021-01-27T12:03:41+00:00 lb100-X15 logger: User acumensec (192.168.254.143) Deleted Intermedidate Certificate PD-IntermediateCA
FIA_X509_EXT.2	None	None	NA
FIA_X509_EXT.3	None.	None.	NA
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None.	2021-10-12T08:58:22+00:00 lb100-X15 logger: User bal (192.168.254.24) Software update started 2021-10-12T09:00:46+00:00 lb100-X15 logger: User bal (192.168.254.24) Installed new software version: 7.2.48.5.21166.RELEASE.20211008-1217 2021-10-12T09:02:01+00:00 lb100-X15 logger: User bal (192.168.254.24) Performed a Reboot 2021-10-12T09:02:01+00:00 lb100-X15 logger: Nosession: Rebooting machine 2021-10-12T09:02:57+00:00 lb100-X15 logger: Nosession: Generated self signed certificate key for 10.1.3.55 2021-10-12T09:02:58+00:00 lb100-X15 logger: Crypto Self-Tests passed 2021-10-12T09:03:01+00:00 lb100-X15 logger: System Booted
FMT_MTD.1/CoreData	None.	None.	NA
FMT_MTD.1/CryptoKeys	None.	None.	NA
FMT_SMF.1	All management activities of TSF data.	None.	• **Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1** **Session establishment through WEBUI:** 2021-02-22T06:53:49+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Logged in (Session: DWAcx7GmQvhDAtXDUdC1cvcz)

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
			Session establishment through Console: 2021-02-22T06:47:34+00:00 lb100-X15 login: pam_unix(login:session): session opened for user bal by LOGIN(uid=0) - **Ability to manage the cryptographic keys:** 2021-02-23T05:35:46+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Logged in (Session: vnfG6vvRYXUisocsmnuH6VUz) 2021-02-23T05:38:00+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Generated a new Self Signed Admin Cert 2021-02-23T05:38:00+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Generated self signed certificate key for 10.1.3.55 - **Ability to configure the cryptographic functionality** 2021-10-12T09:02:01+00:00 lb100-X15 logger: Nosession: Rebooting machine 2021-10-12T09:02:57+00:00 lb100-X15 logger: Nosession: Generated self signed certificate key for 10.1.3.55 - **Ability to administer the TOE locally and remotely** **Session establishment through remotely:** 2022-01-31T13:00:56+00:00 lb100-X15 logger: User acumensec (192.168.254.24) Logged in (Session: Jmzd5lsJGzj4Fz1QdoOkqNkz) 2021-04-07T07:51:12+00:00 lb100-X15 logger: User acumensec (192.168.254.143) set 'NTP_HOST' to '10.1.3.78' 2021-02-23T08:54:05+00:00 lb100-X15 logger: User acumensec (10.1.1.66) set 'INITIAL_AUTH' to 'This is the LOGIN Banner. Authorized users only.'

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
			Session establishment through locally: 2022-01-31T13:12:21+00:00 lb100-X15 bal: lsetup: User bal logged in to session 18C4DB7BB09F from /dev/ttyS0 2022-01-31T13:13:51+00:00 lb100-X15 bal: lsetup: set 'CONSOLE_IDLE' to '600' 2022-01-31T13:15:08+00:00 lb100-X15 bal: lsetup: set 'TRANSFER_MODE' to 'ftp' - **Ability to configure the access banner** **Through WEBUI:** 2021-02-23T08:54:05+00:00 lb100-X15 logger: User acumensec (10.1.1.66) set 'INITIAL_AUTH' to 'This is the LOGIN Banner. Authorized users only.' **Through Console:** 2021-02-23T13:12:41+00:00 lb100-X15 logger: User bal (10.1.1.66) set 'INITIAL_SSH' to 'This is the Console LOGIN banner. WARNING: Authorized users only.' - **Ability to configure the session inactivity time before session termination or locking** **Through WEBUI:** 2021-02-23T05:57:22+00:00 lb100-X15 logger: User acumensec (10.1.1.66) set 'SESSION_IDLE' to '60' **Through Console:** 2021-02-23T13:28:00+00:00 lb100-X15 bal: lsetup: set 'CONSOLE_IDLE' to '60' - **Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates**

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
			2021-10-12T08:58:22+00:00 lb100-X15 logger: User bal (192.168.254.24) Software update started 2021-10-12T09:00:46+00:00 lb100-X15 logger: User bal (192.168.254.24) Installed new software version: 7.2.48.5.21166.RELEASE.20211008-1217 2021-10-12T09:02:01+00:00 lb100-X15 logger: User bal (192.168.254.24) Performed a Reboot 2021-10-12T09:02:01+00:00 lb100-X15 logger: Nosession: Rebooting machine 2021-10-12T09:02:57+00:00 lb100-X15 logger: Nosession: Generated self signed certificate key for 10.1.3.55 2021-10-12T09:02:58+00:00 lb100-X15 logger: Crypto Self-Tests passed • **Ability to configure the authentication failure parameters for FIA_AFL.1** 2021-02-19T09:33:51+00:00 lb100-X15 logger: User bal (10.1.1.66) set 'SESSION_MAXBLOCK' to '3' • **Ability to re-enable an Administrator account** 2021-02-19T09:56:56+00:00 lb100-X15 logger: User bal (10.1.1.66) User acumensec unblocked • **Ability to set the time which is used for timestamps** 2021-04-12T12:12:12+00:00 lb100-X15 logger: User bal (10.1.1.66) Changed time from Mon Apr 12 10:13:45 GMT 2021 to Mon Apr 12 12:12:12 GMT 2021 • **Ability to configure NTP** 2021-04-07T07:51:12+00:00 lb100-X15 logger: User acumensec (192.168.254.143) set 'NTP_HOST' to '10.1.3.78'

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
			• **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors** 2021-04-07T08:04:51+00:00 lb100-X15 logger: User bal (192.168.254.143) Installed an Intermediate Certificate PD-IntermediateCA • **Ability to configure the reference identifier for the peer** 2021-04-07T09:12:09+00:00 lb100-X15 logger: User bal (192.168.254.143) Set Server(s) 10.1.2.241 for LDAP LDAP 2021-04-07T09:16:47+00:00 lb100-X15 logger: User bal (192.168.254.143) Added user test (no password) • **Ability to import X.509v3 certificates to the TOE's trust store** 2021-04-22T05:31:28+00:00 lb100-X15 logger: User bal (192.168.254.143) Installed an Intermediate Certificate PD-IntermediateCA 2021-04-22T06:15:23+00:00 lb100-X15 logger: User bal (192.168.254.143) Added certificate 10.1.3.55_384
FMT_SMR.2	None.	None.	NA
FPT_SKP_EXT.1	None.	None.	NA
FPT_APW_EXT.1	None.	None.	NA
FPT_TST_EXT.1	None.	None.	NA
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.	2021-10-12T08:58:22+00:00 lb100-X15 logger: User bal (192.168.254.24) Software update started 2021-10-12T09:00:46+00:00 lb100-X15 logger: User bal (192.168.254.24) Installed new software version: 7.2.48.5.21166.RELEASE.20211008-1217 2021-10-12T09:02:01+00:00 lb100-X15 logger: User bal (192.168.254.24) Performed a Reboot

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
			2021-10-12T09:02:01+00:00 lb100-X15 logger: Nosession: Rebooting machine 2021-10-12T09:02:57+00:00 lb100-X15 logger: Nosession: Generated self signed certificate key for 10.1.3.55 2021-10-12T09:02:58+00:00 lb100-X15 logger: Crypto Self-Tests passed
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	**Manual Setting of Time:** 2021-04-12T12:12:12+00:00 lb100-X15 logger: User bal (10.1.1.66) Changed time from Mon Apr 12 10:13:45 GMT 2021 to Mon Apr 12 12:12:12 GMT 2021 **Setting of time using NTP:** 2021-03-01T06:03:59+00:00 lb100-X15 logger: User bal (10.1.1.66) Set Time from NTP server "10.1.3.78" to Mon Mar 1 06:03:59 UTC 2021 from Mon Mar 1 06:03:51 UTC 2021 2021-03-01T06:04:00+00:00 lb100-X15 logger: User bal (10.1.1.66) set 'NTP_HOST' to '10.1.3.78'
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism.	None.	2021-02-23T13:31:59+00:00 lb100-X15 login: pam_unix(login:session): session closed for user bal
FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None.	2021-02-23T06:08:05+00:00 lb100-X15 logger: User acumensec Timed out (Session : 0fSP61aY028Yx4MzMdb1Imcz)
FTA_SSL.4	The termination of an interactive session.	None.	**Console:** 2021-02-23T06:47:56+00:00 lb100-X15 login: pam_unix(login:session): session closed for user bal **WEBUI:** 2021-02-23T07:02:34+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Logged out (Session: M2XLqpABnoDrb1vENb9qT1kz)
FTA_TAB.1	None.	None.	NA
FTP_ITC.1	- Initiation of the trusted channel.	Identification of the initiator and target of failed trusted channels	**Initiation of the trusted channel:** 2021-04-07T07:05:59+00:00 lb100-X15 syslog-ng: Syslog connection established; server='10.1.3.78'

Requirement	Auditable Events	Additional Audit Record Contents	Sample Logs
	• Termination of the trusted channel. • Failure of the trusted channel functions.	establishment attempt.	**Termination of the trusted channel:** 2021-04-07T07:28:22+00:00 lb100-X15 syslog-ng: Syslog connection broken; server='10.1.3.78', time_reopen='60' **Failure of the trusted channel:** 2021-01-11T07:00:43+00:00 lb100-X15 validuser: do_ldap_check: ldap_sasl_bind_s(): rc=-1, bind failed for user [acumensec], error: error:1409017F:SSL routines:ssl3_get_server_certificate:wrong certificate type
FTP_TRP.1/Admin	• Initiation of the trusted path. • Termination of the trusted path. • Failure of the trusted path functions.	None.	**Initiation of the trusted path:** 2021-02-23T07:04:07+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Logged in (Session: V427Nl3msSNtFQ29k4glj3Mz) **Termination of the trusted path:** 2021-02-23T07:02:34+00:00 lb100-X15 logger: User acumensec (10.1.1.66) Logged out (Session: M2XLqpABnoDrb1vENb9qT1kz) **Failure of the trusted path functions:** 2021-02-10T08:16:39+00:00 lb100-X15 sslproxy: Failing client cert (err certificate signature failure) (Serial Number 7633981780902228442) /C=US/O=Acumen/OU=CC/CN=PD-IntermediateCA.acumensec.local 2021-02-10T08:16:39+00:00 lb100-X15 sslproxy: Client 10.1.1.66 failed SSL negotiation (crypto/asn1/a_verify.c/162): error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib)

6. References

Link to UI Guide:

https://support.kemptechnologies.com/hc/en-us/articles/213906303-Web-User-Interface-WUI-

Link to CLI guide:

https://support.kemptechnologies.com/hc/en-us/articles/203128129-Command-Line-Interface-CLI-

Link to Procuring the TOE:
Latest Firmware – Kemp Support (kemptechnologies.com)