MAGNUM-HW-CC Security Administration Manual for Common Criteria

MAGNUM-HW-CC SDVN 21.10

Revision 03, January 13, 2023

EVERTZ MICROSYSTEMS LTD.
5292 John Lucas Drive
Burlington, Ontario
Canada L7L5Z9

Phone:	+1 905-335-3700		
Sales:	sales@evertz.com	Fax:	+1 905-335-3573
Tech Support:	service@evertz.com	Fax:	+1 905-335-7571
Web Page:	www.evertz.com	Twitter:	@EvertzTV

This page left intentionally blank

Contents

This page left intentionally blank

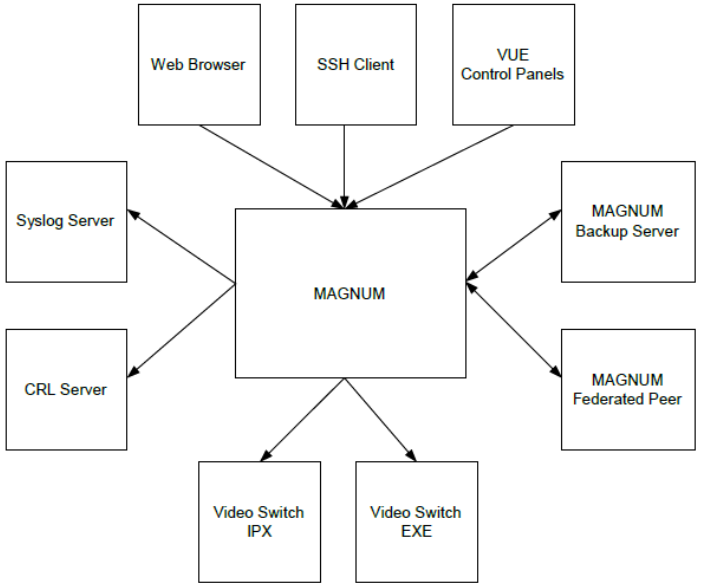
1. OVERVIEW

This manual is a supplement to the “MAGNUM-HW User Manual v2.2.” It is specifically intended for use with the MAGNUM-HW-CC. MAGNUM is a software product produced by Evertz. MAGNUM-HWC-CC is a product consisting of MAGNUM software pre-installed on an Evertz-provided server. MAGNUM-HW-CC is a product that meets the “Collaborative Protection Profile for Network Devices” for “Common Criteria.”

MAGNUM-HW-CC only meets these requirements in “High Security Mode.” It is shipped with the security mode turned off (“Normal Security Mode”). Customers can choose to use only a subset of the “High Security Mode” features. (Evertz does not recommend using only a subset of “High Security” features; MAGNUM is not in its evaluated configuration unless placed into “High Security Mode”.) Once “High Security Mode” is enabled it is permanent. To be clear, MAGNUM-HW-CC only meets the “Collaborative Protection Profile for Network Devices” for “Common Criteria” when in “High Security Mode” and should be used in this configuration.

Except where specifically stated in this manual the nature of physical network connections is outside the scope of the “Collaborative Protection Profile for Network Devices” for “Common Criteria,” as the available network elements (IP switches, IP routers, etc.) which may be used in establishing those links are site-specific. Evertz stipulates that any connection must meet organization-specific security requirements for the location(s) where the equipment is deployed. MAGNUM-HW-CC is recommended to be deployed in a closed network.

The following diagram shows typical MAGNUM connections:


Web Browser
SSH Client
VUE
Control Panels
Syslog Server
MAGNUM
MAGNUM
Backup Server
CRL Server
MAGNUM
Federated Peer
Video Switch
IPX
Video Switch
EXE

2. INITIAL SETUP

2.1. Obtaining and installing the CC Certified Firmware

Secure Delivery Verification

Before installing the Evertz Magnum unit, you should take steps to ensure the unit has not been tampered with during transit. Perform the following checks to verify the integrity of the unit prior to installation.

1. Courier - Evertz only uses bonded couriers such as UPS, FedEx or DHL. Verify the shipment was received using a bonded courier.
2. Shipping information - Verify the shipment information against the original purchase order or evaluation request.
3. Verify the shipment has been received directly from Evertz.
4. External packaging - Verify the Evertz branded packing tape sealing the packaging is intact and the packaging has not been cut or damaged to allow access to the unit.
5. Internal packaging - Verify the unit is sealed in an undamaged. verify the internal box packaging is intact.
6. Warranty seal - Verify the unit's warranty seal is intact. The chassis cannot be opened without destroying the warranty seal.

If you identify any concerns while verifying the integrity of the unit, contact your supplier immediately.

Device Registration

Once the product is received and secure delivery is ensured, contact the Evertz sales team to register the product.

Physical security Requirements

Common Criteria compliant operation requires that you use the Magnum Server in its HIGH Security mode of operation and that you follow secure procedures for installation and operation of the unit. You must ensure that:

1. The Magnum Server is installed in a secure physical location.

2. Physical access to the Magnum Server unit is restricted to authorized operators.

Installing the unit

The documentation shipped with your unit includes a Start Guide and a model specific Hardware Supplement. The configuration guides, user guides, and administrative guides can be obtained after registering the product online.

Downloading the CC certified firmware

The validated firmware version is 21.10.4.

The MAGNUM server is typically deployed in a closed network without direct access to the internet. In these instances, Administrators are required to contact Evertz to receive notification of production updates directly or via email blast. Operators may verify the current version using the CLI menu 'Version' or on the web interface Config Management->Current System Info.

Customers requiring secure delivery for site policy can request secure courier delivery of software updates. Digital delivery may be provided via File Transfer Protocol Secure (FTPS) using signed and hashed code.

The following steps are required after the first boot to put MAGNUM into the Common Criteria evaluated configuration:

1. Observer Power-On Self Test passage
2. Configure IP addresses
3. Configure the Date, Time, and Time Zone
4. Enable High Security Mode
5. Remove the Evertz default CRL and CA
6. Import the organization's CAs and CRLs
7. Configure Secure Audit Servers

Details of all functions that are configured in High Security Mode can be found in Section 14. High Security Mode sets all cryptographic configurations for the TOE, including limiting cryptographic parameters to only the following:

- Ciphersuites allowed for TLS:
    - TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268
    - TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268
    - TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246
    - TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

- SSH cryptographic configurations:
    - AES CTR with 128-bit or 256-bit keys for encryption
    - SSH-RSA, RSA-SHA2-256, and RSA-SHA2-512 for authentication
    - ECDH-SHA2-NISTP256, ECDH-SHA2-NISTP384, ECDH-SHA2-NISTP512 for key exchange
    - HMAC-SHA2-256 and HMAC-SHA2-512 for SSH transport MAC algorithms

- TLS Key establishment is performed with either RSA or ECDHE. The selection between key establishment schemes is determined by the TLS ciphersuite selection.
- SSH supports key exchange using ecdh-sha2-nistp256, ecdh-sha2-nistp521, or ecdh-sha2nistp384 as selected by the SSH client.

The TOE does not allow any configuration of cryptographic parameters other than entering and exiting High Security Mode. All other cryptographic parameters are set and cannot be changed including:

- Random number generation using AES-256 CTR DRBG with SHA-256 hash
- Key generation of RSA 4096-bit keys to support digital signatures
- ECDSA keys with NIST curves P-256 or P-384 to support ECDHE key agreement
- SHA-512 used to verify file checksums and hash stored passwords
- HMAC-SHA-1/256/384/512 used for TLS and SSH sessions and verification of firmware image
- SSH rekey thresholds of 1 hour or 1 GB of data

- Reject any SSL connection or TLS v1.0 or v1.1 connections

3. ADMINISTERING THE MAGNUM

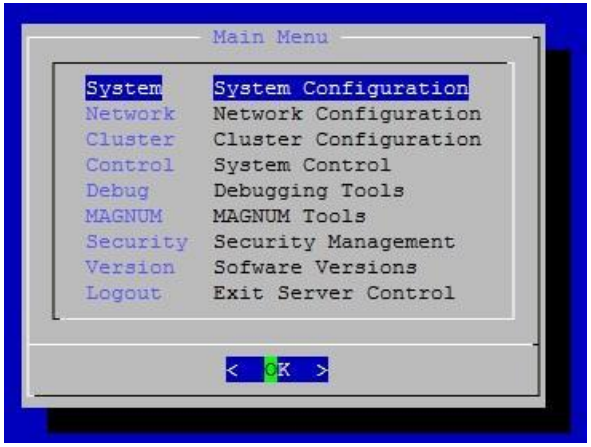
Only the authorized security administrators can perform the administrative tasks.

3.1. Local Console

Logging in to Local Console

Most administrative actions are accomplished through the console menu. Failed login attempts on the local console **do not** trigger account lockouts. Only administrative users have access to the console menu, either locally or remotely. No unprivileged users are permitted access to the console menu.

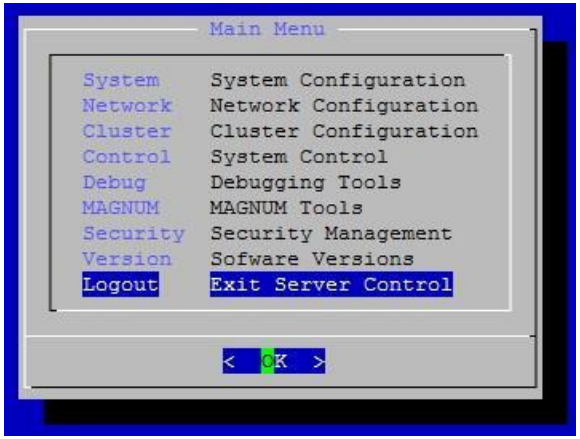
1. Connect a VGA monitor and a USB keyboard
2. Switch console sessions by pressing <CTRL><ALT><F1> through <CTRL><ALT><F6>.
3. Log in with username **configshell** and default password **configshell** to access a structured menu



4. Changing any settings requires entering **configshell**'s password each time, and that step is assumed in all instructions. Security-sensitive changes are further protected by user prompts and warnings.
5. There also exists users **etservice** and **etdev** that access an open shell with limited permissions

Logging Out of Local Console

1. Select **logout** at the bottom of the menu list



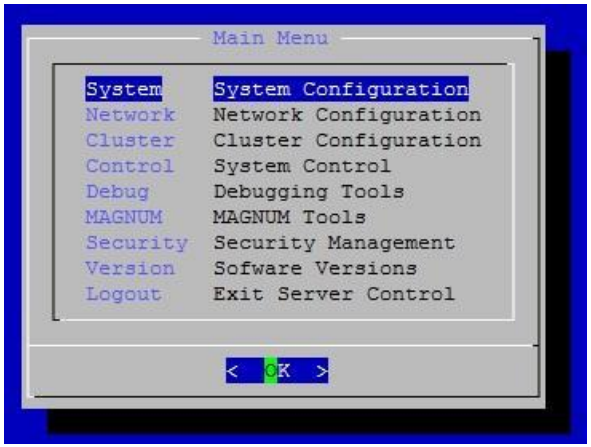
2. This will close the current administration session

3.2. SSH

Logging in with SSH

The console menu is available over SSH for remote administration. Too many failed login attempts over SSH will trigger account lockouts.

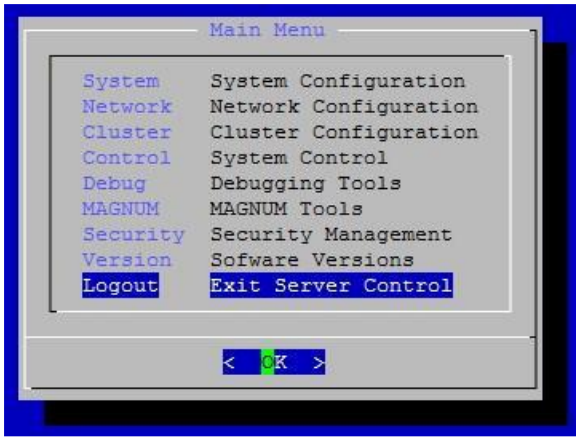
1. Use Putty or a similar SSH client from a PC
2. Enter MAGNUM's IP address (use default port 22)
3. Log in with username **configshell** and default password **configshell** to access a structured menu



4. Changing any settings requires entering **configshell**'s password each time, and that step is assumed in all instructions. Security-sensitive changes are further protected by user prompts and warnings.
5. There also exists users **etservice** and **etdev** that access an open shell with limited permissions

Logging out of SSH

1. Select **logout** at the bottom of the menu list



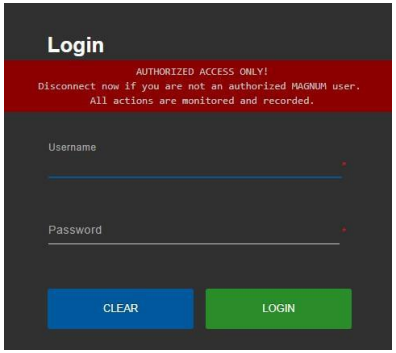
2. This will close the current SSH session

3.3. Web Interface

Logging in to Web Interface

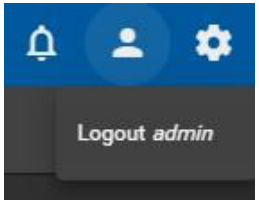
MAGNUM's application features are accessed with a web browser. Security Administrators can securely administer the Magnum via Web Graphical User Interface once the IP address is configured, and a valid Server Certificate is imported. The steps to configure IP address and certificate management can be found in section 8 and section 14.
Chrome and Safari Web Browsers are supported. The ciphersuites the browser should support to obtain successful connectivity with the Magnum's HTTPS server is listed in section 2 above. Too many failed logins over the web interface will trigger account lockouts.

1) Open a supported web browser
2) Enter the IP address of MAGNUM
3) Log in with username admin and default password admin (other users can be created as well)



Logging out of Web Interface

1. Select the **person icon** on the top right of the web page



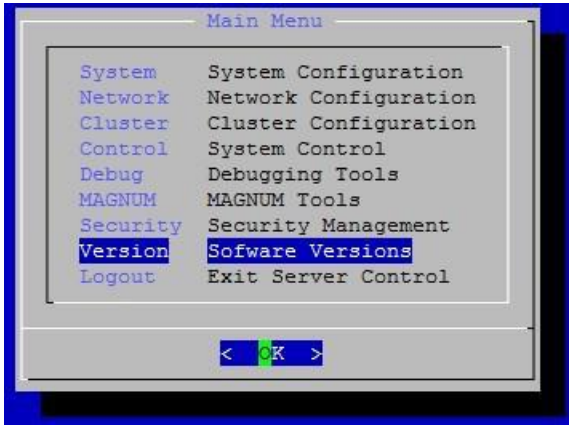
2. Select Logout

4. UPGRADING THE FIRMWARE

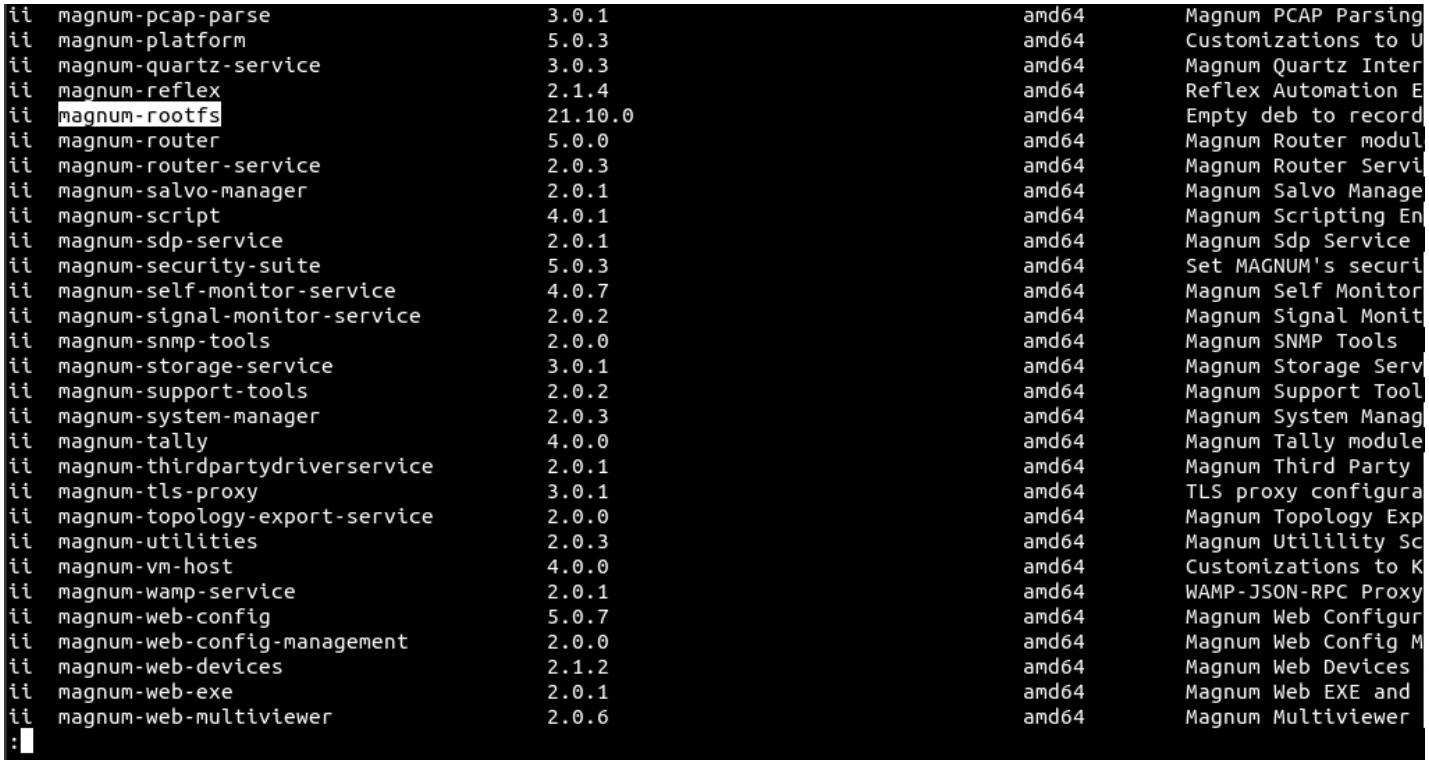
4.1. Check Firmware Version

Check version from Console

1. Log in to the console as **configshell**
2. Select Version



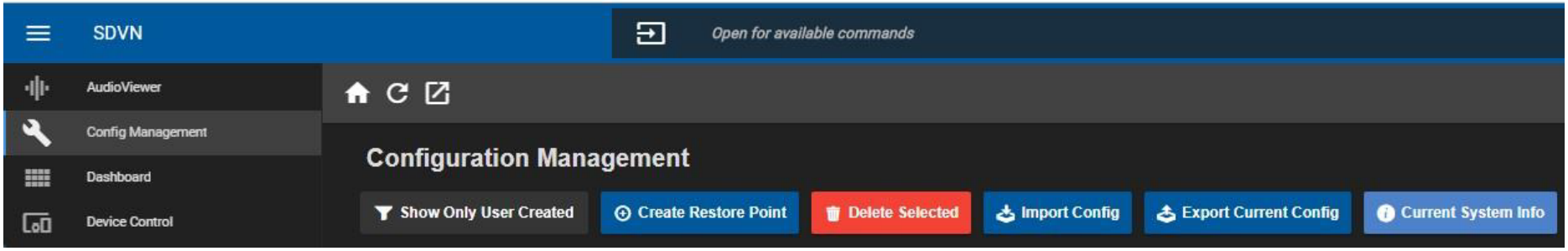
3. Using the arrow keys, scroll through the installed packages list
4. Search by entering **/** (forward slash) then a search pattern
5. Search for “magnum-rootfs” to get the MAGNUM version



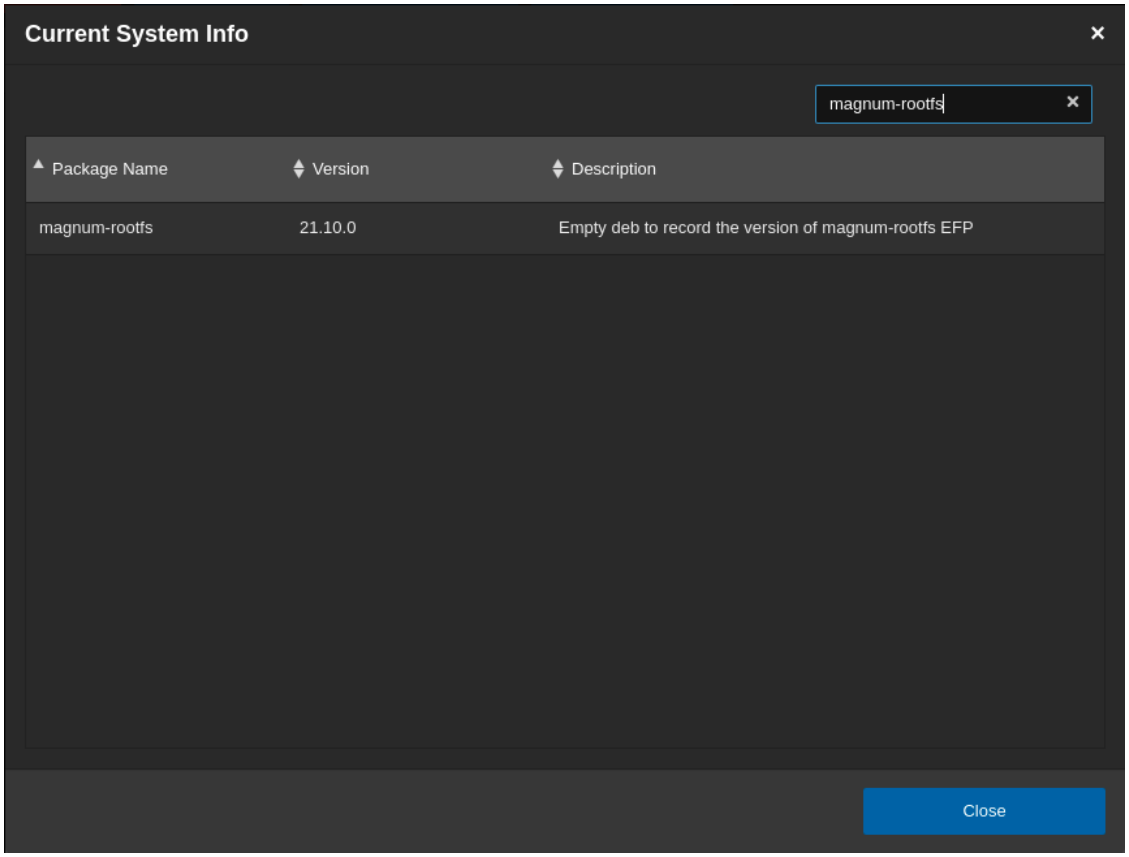
6. Press the **q** key to return to the main menu

Check Version from Web Interface

1. Log in to the web interface as admin
2. Select Configuration Management from the SDVN system
3. Select Current System Info



4. Scroll or search for “magnum-rootfs” to get the MAGNUM version

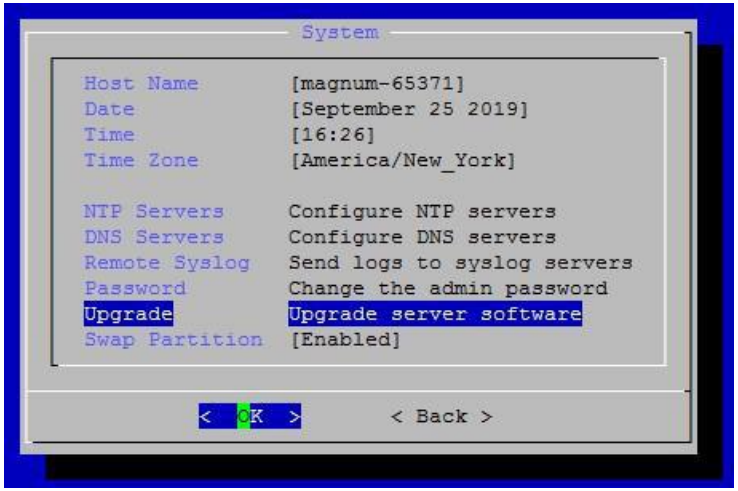


5. Click Close

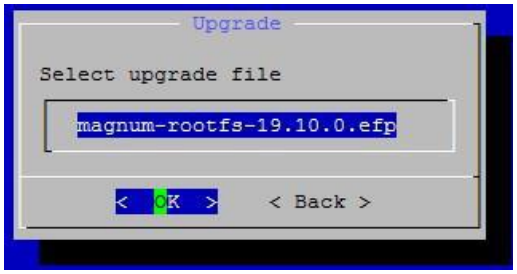
4.2. Performing Firmware Upgrade

Administrators are required to contact Evertz to receive notifications of product updates directly or via an email blast. In High Security Mode, all firmware upgrade images (.efp files) will have their signatures (.sig files) verified before being installed. Evertz signs these firmware images at build-time. If the .efp file has been tampered with, the installation is aborted. Always keep the .sig file beside the .efp file.

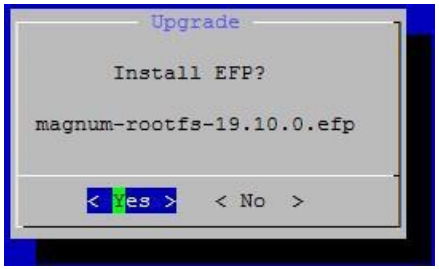
1. Log in to the console as configshell and select System
2. Select Upgrade



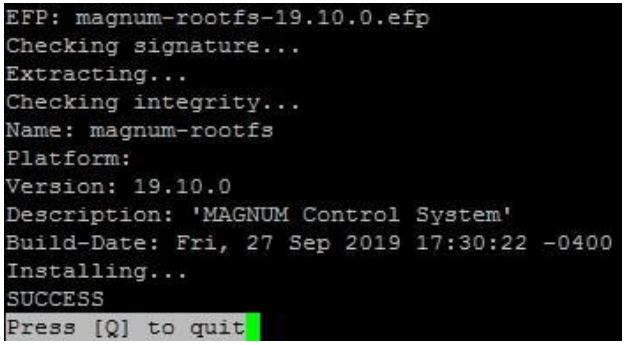
3. When prompted, enter configshell's password
4. Select the file's source, either /home/configshell via SFTP or USB Device
5. Select the correct .efp file (the .sig file won't appear but it is expected to be beside the .efp file)



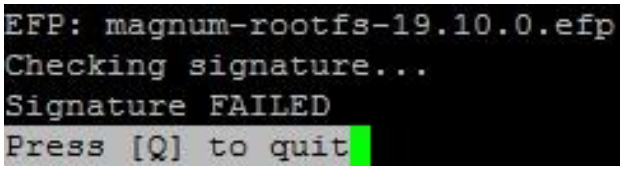
6. Consider the prompt, and select Yes to proceed



7. When prompted, enter configshell's password
8. Wait until the upgrade completes, and press q to return



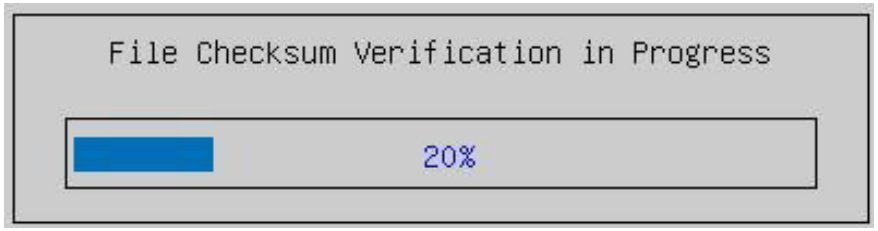
9. When prompted, reboot
10. If the EFP is corrupted it will display the following message:



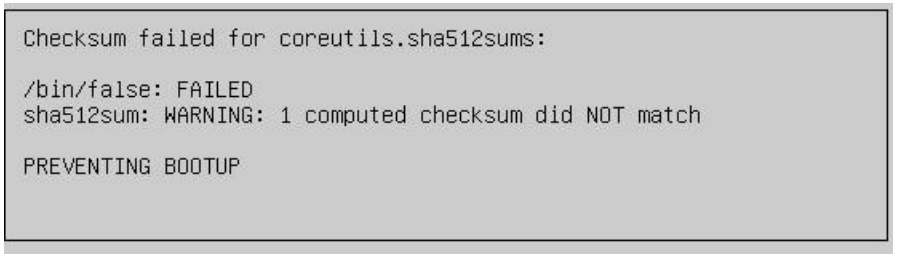
11. If the upgrade fails, contact Evertz Service Department

4.3. Firmware Integrity Check

In High Security Mode, a firmware integrity check is performed at every power-on:



If the firmware integrity check fails (as shown here), please contact the Evertz Service Department.



5. SYSTEM SECURITY MODE

The device should not be considered online, and should not be connected to the network, unless it is in High Security Mode. Putting the device in High Security Mode configures the TLS ciphers and all other cryptographic engine requirements needed in the evaluated configuration. No other configuration of cryptography is permitted on the TOE. The TOE was evaluated in High Security Mode, with the cryptographic configurations permitted within this mode. The use of other cryptographic engines was not tested or evaluated and therefore should not be used.
These are the changes when entering High Security Mode:

1. Set new passwords for console users (configshell, etdev, etservice)
2. Expire all web user passwords (set new password at each user's next successful login)
3. Securely erase and regenerate all keys (SSH and TLS)
4. Set security options according to this table (changing any puts MAGNUM into Custom security mode):

Security Option	**Normal Security Mode**	**High Security Mode**
Ability for etdev to sudo	Enabled	Disabled
Account Lockout Duration	15 min	15 min
Account Lockout Threshold	10 min	10 min
Firmware Integrity Check	Disabled	Enabled
Minimum Password Length	4	8
Password Complexity	Disabled	Enabled
Session Timeout	60 min	15 min
Web Login Banner	Disabled	Enabled

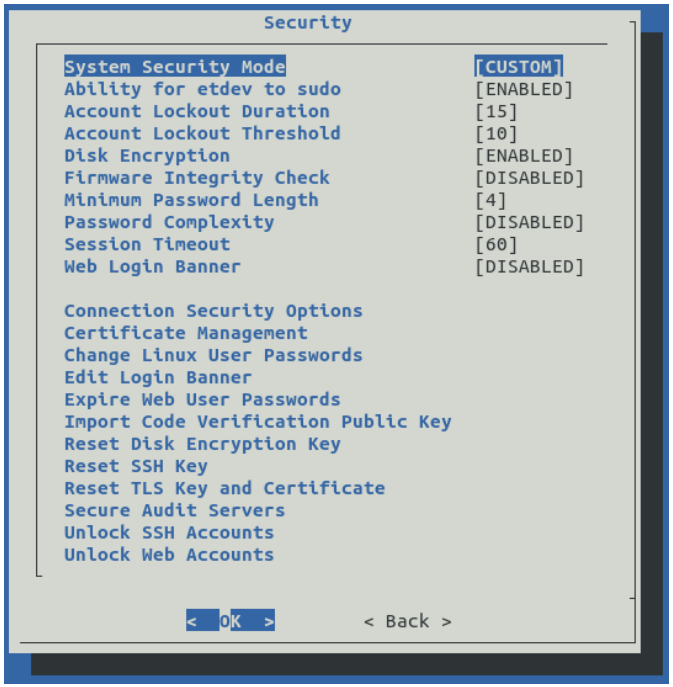
5. Set connection security options according to this table (changing any puts MAGNUM into Custom security mode):

Connection Type	**Port and Direction**	**Normal Security Mode**	**High Security Mode**
SSH Server	22 in	unblocked	unblocked
SSH Client	22 out	unblocked	unblocked
SNMP Agent Gets	161 in	unblocked	blocked

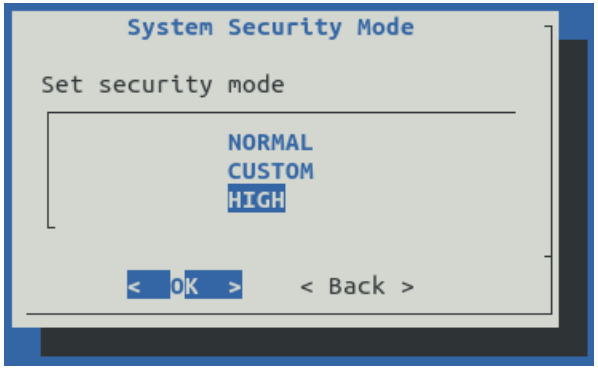
SNMP Agent Traps	162 out	unblocked	blocked
LDAP Authentication	389 out	unblocked	blocked
Web Server	443 in	unencrypted	encrypted
Rsync Replication	873 in	encrypted	encrypted
Rsync Replication	873 out	encrypted	verify-cert-and-crl
Quartz Interfaces	4000-4009 in	unencrypted	encrypted
Remote Syslog	6514 out	encrypted	verify-cert-and-crl
RPC Devices	6577 out	unencrypted	verify-cert-and-crl
Authentication Service	8210 in	encrypted	encrypted
IPX/EXE Devices	9672 out	unencrypted	verify-cert-and-crl
JSON-RPC Devices	9677 out	unencrypted	verify-cert-and-crl
VIP Devices	9700 out	unencrypted	verify-cert-and-crl
VUE/vScribe	9720 out	unencrypted	verify-cert-and-crl

To enable High Security Mode:

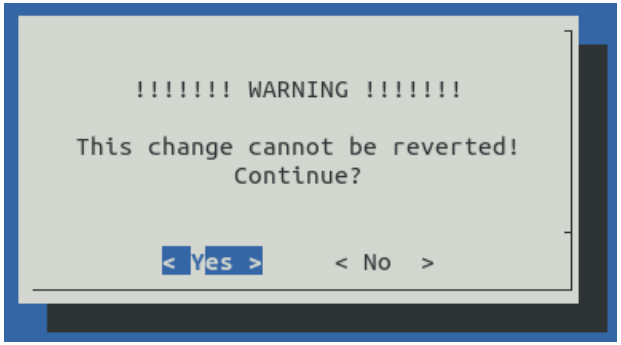
1. Log in to the console as **configshell** and select **Security**



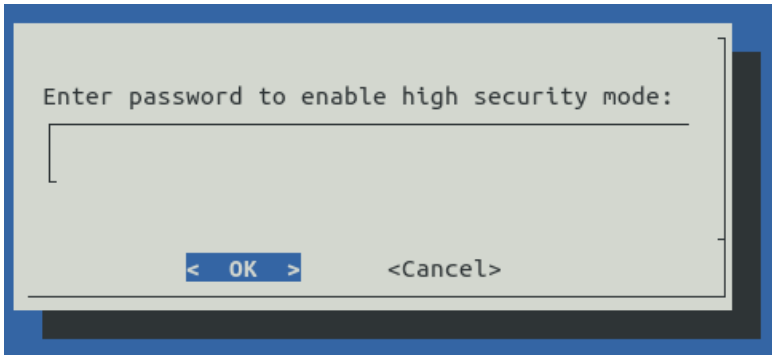
2. Select **System Security Mode** and then **HIGH**



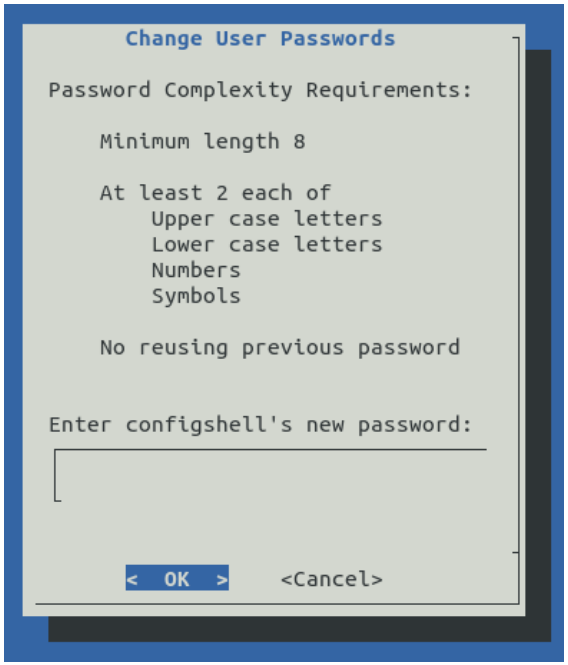
3. Select **Yes** to acknowledge that entering High Security Mode is permanent



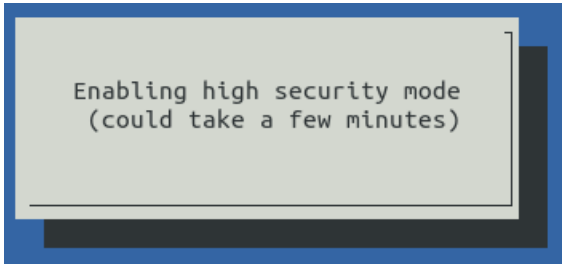
4. When prompted, enter **configshell**'s password



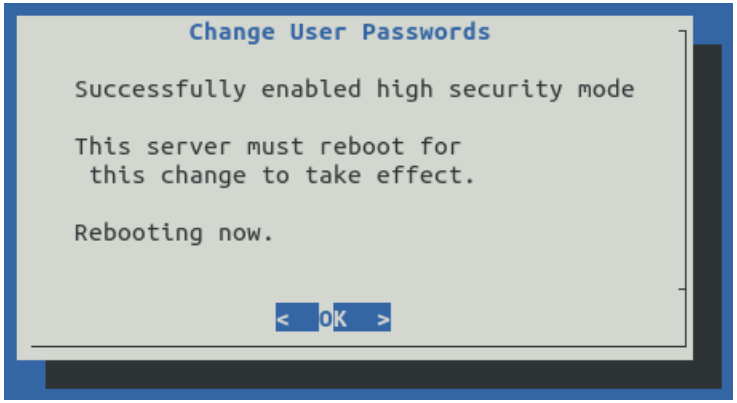
5. Set a new password for each console user (configshell, etdev, etservice), subject to increased password complexity requirements. An internal user "postgres" also uses a password that needs to be changed. All MAGNUM devices in a cluster must use the same "postgres" user password.



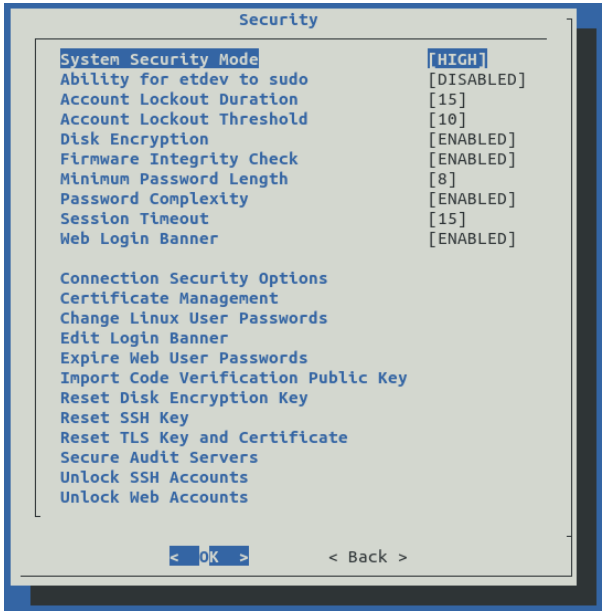
6. Web user passwords are automatically expired and each user will be forced to change their password at their next successful login
7. Wait while the device enables High Security Mode



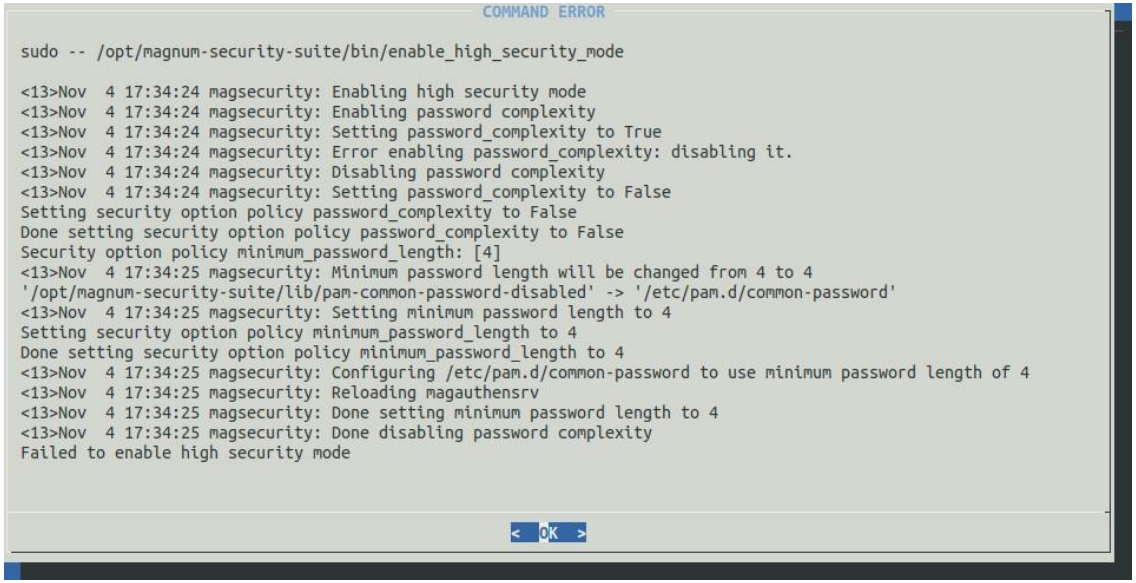
8. When prompted, reboot



9. MAGNUM will now reboot into High Security Mode



If an error occurs with any setting when entering High Security Mode, an error will be shown for the specific setting followed at the end by a warning ‘Failed to enable high security mode’.



If an error occurs, the administrator should reset High Security Mode. If the error does not clear, contact Evertz support for assistance.

5.1. Connection Security Options

When entering High Security Mode, the following connection security options are set (changing any puts MAGNUM into Custom Security Mode):

Connection Type	Port and Direction	Normal Security Mode	High Security Mode
SSH Server	22 in	unblocked	unblocked
SSH Client	22 out	unblocked	unblocked
SNMP Agent Gets	161 in	unblocked	blocked
SNMP Agent Traps	162 out	unblocked	blocked

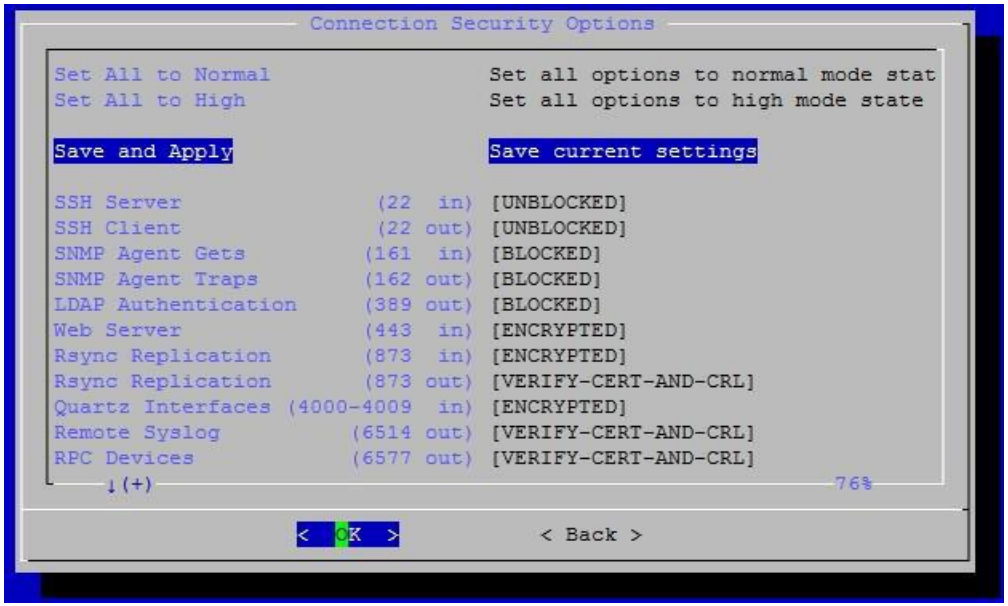
LDAP Authentication	389 out	unblocked	blocked
Web Server	443 in	unencrypted	encrypted
Rsync Replication	873 in	encrypted	encrypted
Rsync Replication	873 out	encrypted	verify-cert-and-crl
Quartz Interfaces	4000-4009 in	unencrypted	encrypted
Remote Syslog	6514 out	encrypted	verify-cert-and-crl
RPC Devices	6577 out	unencrypted	verify-cert-and-crl
Authentication Service	8210 in	encrypted	encrypted
IPX/EXE Devices	9672 out	unencrypted	verify-cert-and-crl
JSON-RPC Devices	9677 out	unencrypted	verify-cert-and-crl
VIP Devices	9700 out	unencrypted	verify-cert-and-crl
VUE/vScribe	9720 out	unencrypted	verify-cert-and-crl

If any outgoing client connections are unintentionally broken, MAGNUM will automatically reconnect within seconds.
There are six possible states for each port:

- unblocked: UDP or TCP port is unblocked
- blocked: UDP or TCP port is blocked by internal firewall
- unencrypted: TCP connections on this port will be plaintext (no TLS)
- encrypted: TCP port uses TLS without certificate checking
- verify-cert: TCP port uses TLS and verifies peer's certificate chain against trusted CAs
- verify-cert-and-crl: TCP port uses TLS and verifies peer's certificate chain including CRLs

If needed, it is possible to reconfigure a port's state:

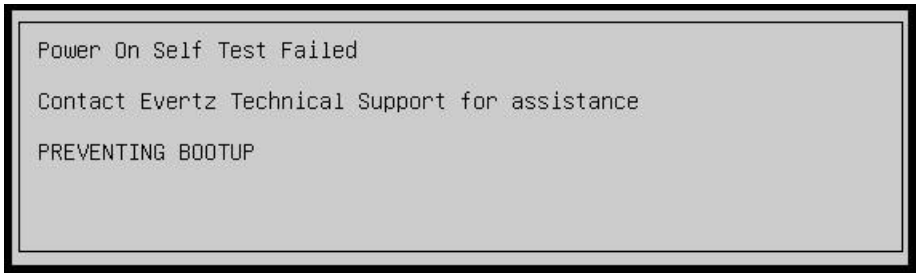
1) Log in to the console as configshell and select Security
2) Select Connection Security Options



3) Configure ports as required and select Save and Apply

5.2. Power-On Self-Test

A self test of the device's cryptographic modules is always performed at power-on. If Cryptographic tests fails, the Magnum will stop bootup and the following message will be displayed for the users on Console.

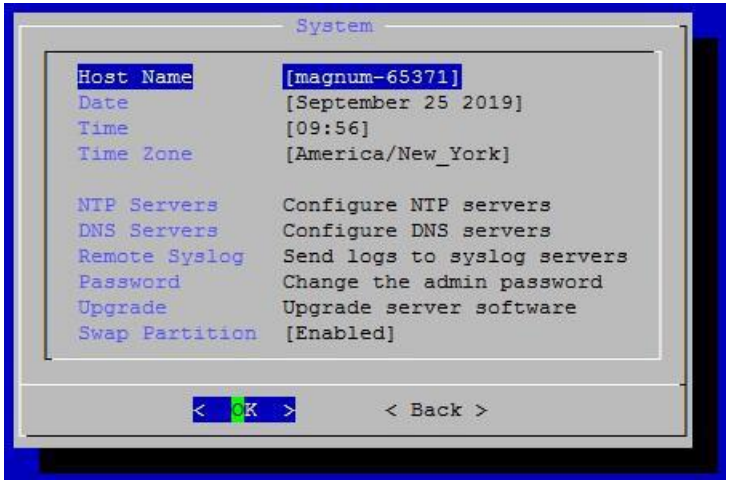


If the self test failure is detected, please contact the Evertz Service Department

6. CONFIGURING DATE AND TIME

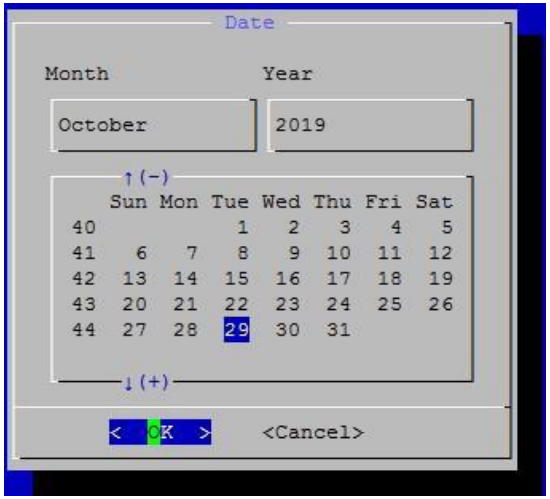
Understanding logged audit events requires accurate time keeping. Reboot is required after changing the date or time.

1. Log in to the console as **configshell** and select **System**

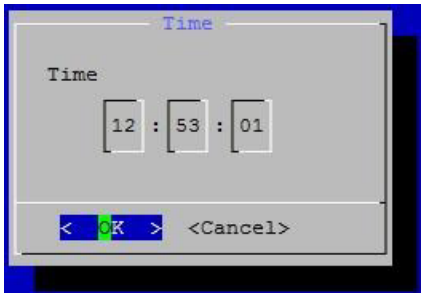


2. Select and configure Time Zone

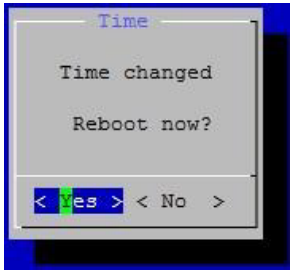
3. Select and configure Date



4. Select and configure Time


Time
Time
12 : 53 : 01
< OK > <Cancel>

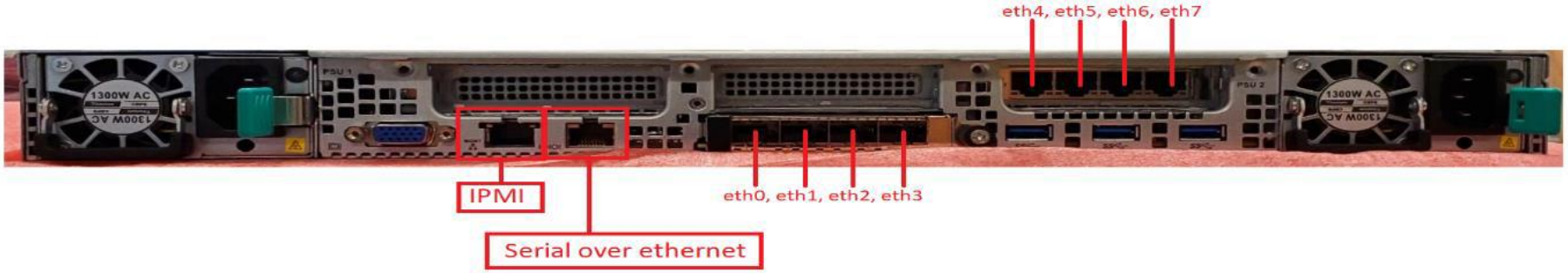
5. Reboot


Time
Time changed
Reboot now?
< Yes > < No >

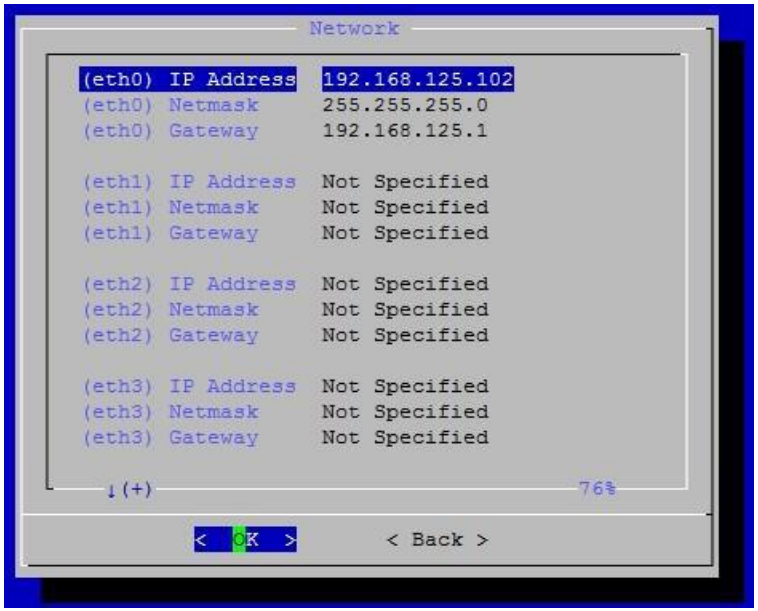
7. CONFIGURING IP ADDRESSES

MAGNUM is usually given static IP addresses. There are multiple network ports, configured differently depending on each organization's requirements.

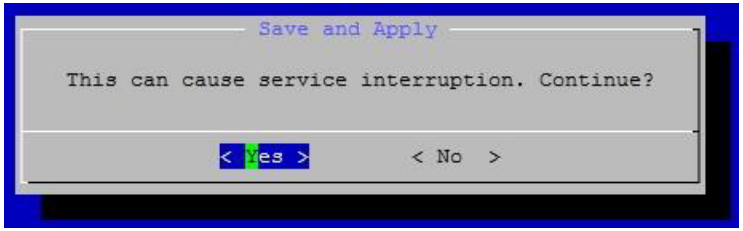
1. These are the port names on the MAGNUM device:



2. Log in to the console as **configshell** and select **Network**
3. Assign **IP Addresses** (and **Gateways** if needed) to the appropriate network ports



4. If the organization requires redundant network links, team ports by creating a “bond”
5. Select **Save and Apply** at the bottom
6. When prompted, select Yes to tolerate the service interruption

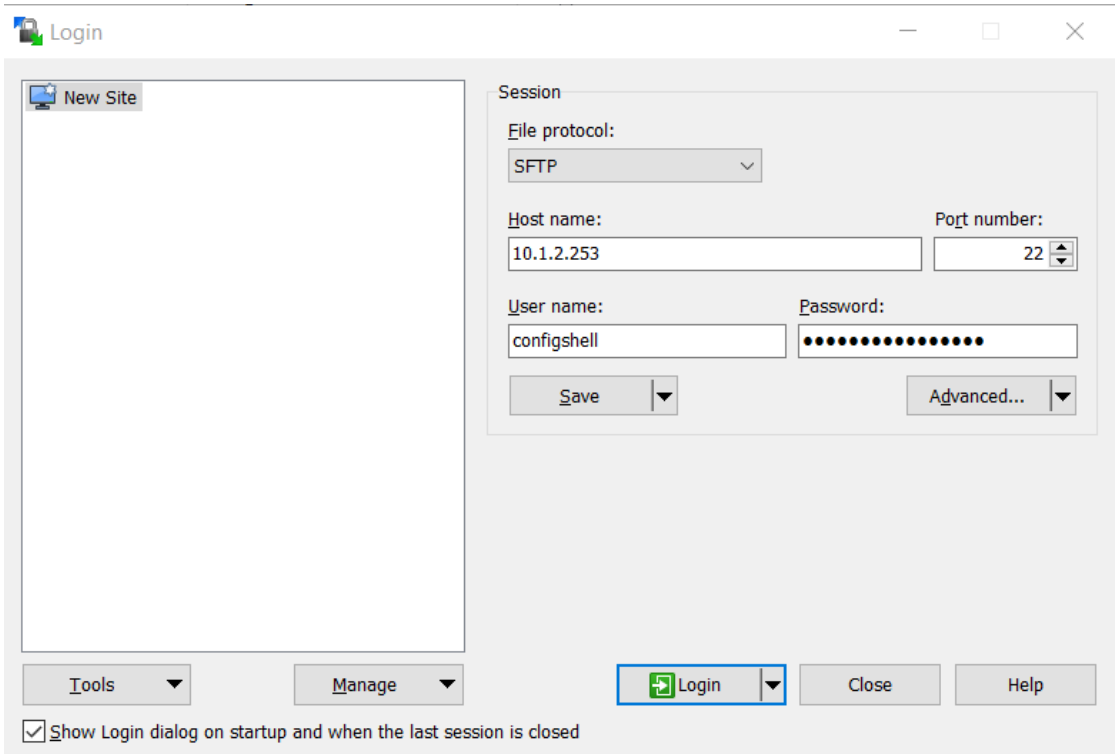


8. TRANSFER FILES

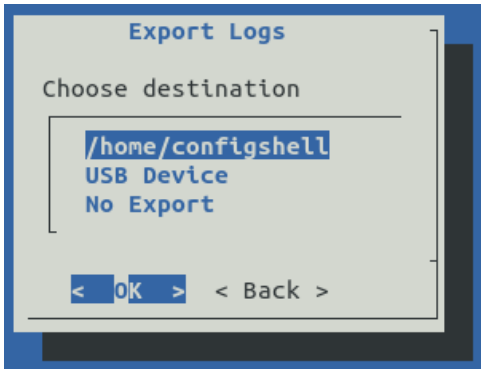
8.1. Transfer files using SFTP

Many menu options require transferring files to or from the device. The admin user requires SFTP.

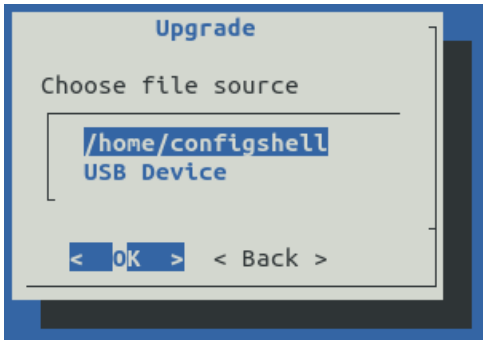
1. Use WinSCP or a similar SFTP client from a PC
2. Enter MAGNUM's IP address and login credentials for admin



3. Use the client's interface to transfer files
4. When exporting files, select /home/configshell as the destination



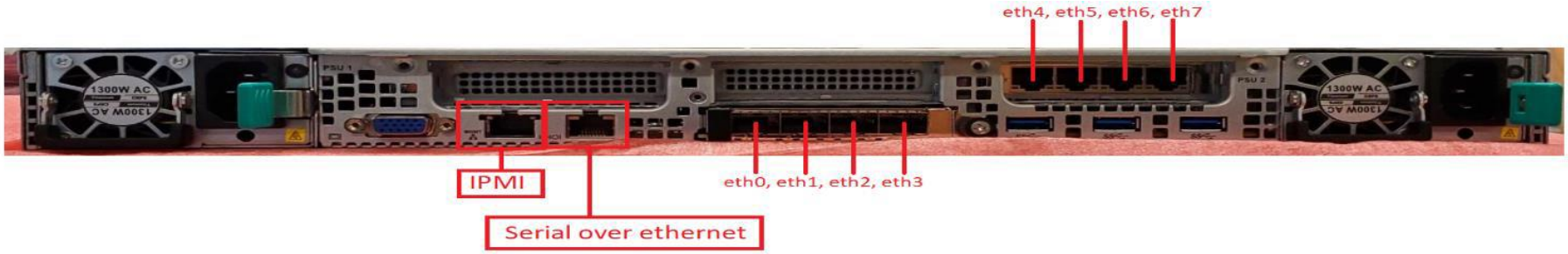
5. When importing files, select /home/configshell as the source



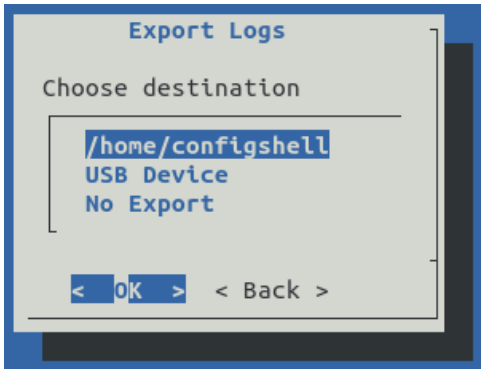
8.2. Transfer files using USB Drive

Many menu options require transferring files to or from the device. USB drives formatted with NTFS and FAT are supported.

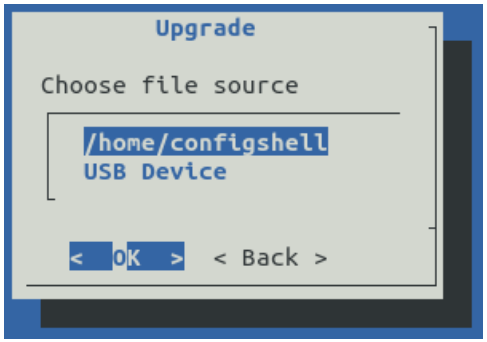
1. USB ports are on the back of the device:



2. When exporting files, select USB Device as the destination



3. When importing files, select **USB Device** as the source


Upgrade
Choose file source
/home/configshell
USB Device
< OK >
< Back >

9. ADMINISTRATIVE FUNCTIONS

Among many administrative functions, the Security Administrators can perform the following management functions. All the following security functions are restricted to authorized security administrators.

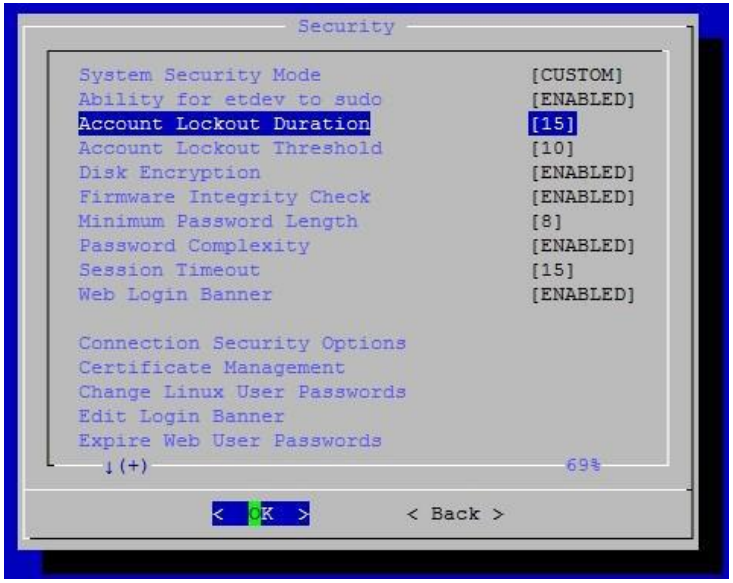
- Audit configuration
- Administer the TOE locally and remotely.
- Configure the authentication failure parameters.
- Update the Magnum, and to verify the updates using digital signature capability prior to installing those updates.
- Resetting passwords.
- Administrative login and logout.
- Generate CSRs, import x509 certificates, and delete x509 certificates.
- Configure the access banner.
- Configure the session inactivity time before session termination or locking.
- Configure remote audit server parameters.
- Set the time which is used for time-stamps.

10. USER AUTHENTICATION FAILURE PARAMETERS

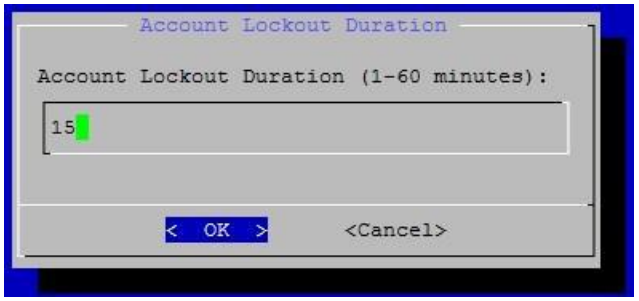
10.1. Account Lockout Duration

Configure how long console and web accounts are locked after too many failed login attempts.

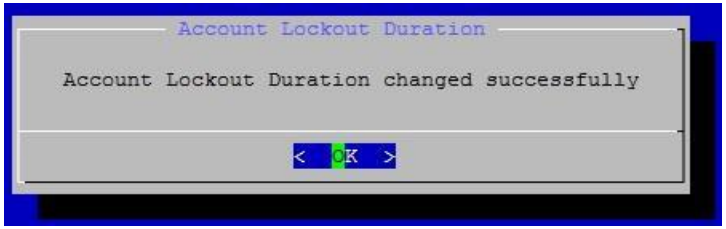
1. Log in to the console as configshell and select Security



2. Select Account Lockout Duration
3. When prompted, enter configshell's password
4. Enter the new account lockout duration (in minutes)



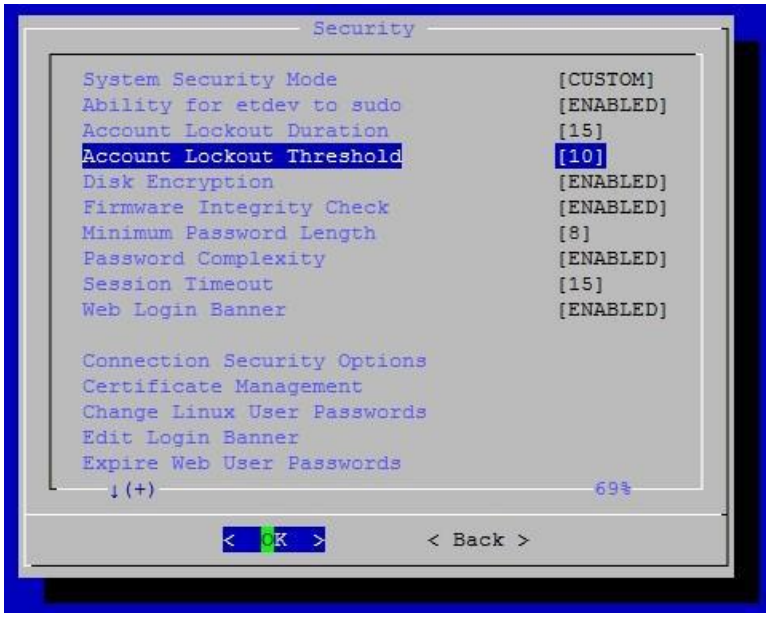
5. The change will take effect immediately



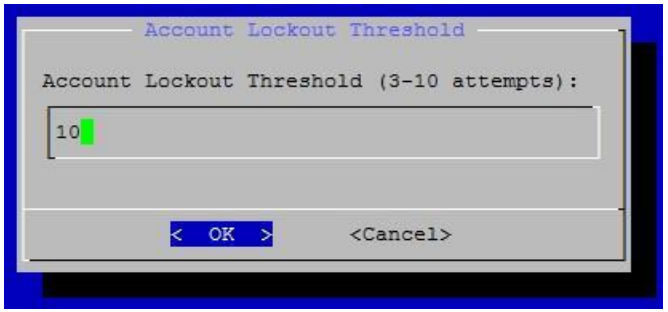
10.2. Account Lockout Threshold

Configure how many failed login attempts will temporarily lock console and web accounts

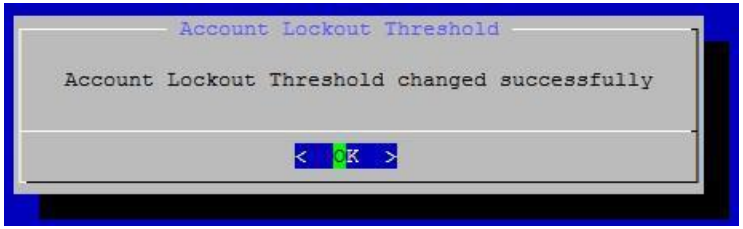
1. Log in to the console as configshell and select Security



2. Select Account Lockout Threshold
3. When prompted, enter configshell's password
4. Enter the new account lockout threshold



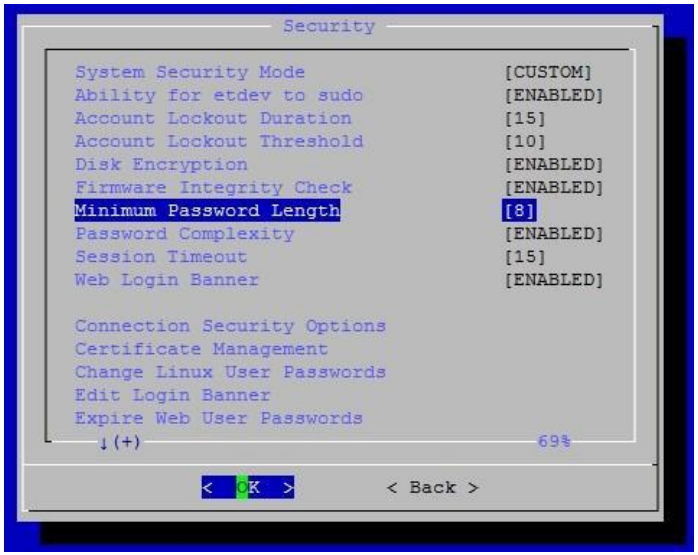
5. The change will take effect immediately



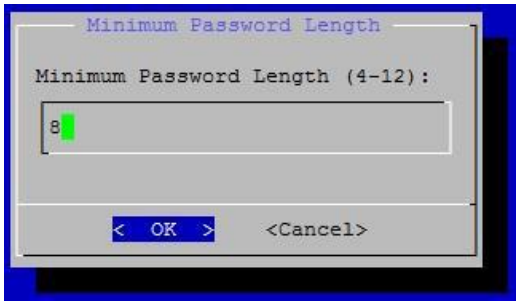
10.3. Minimum Password Length

Configure the minimum password length for console and web users.

1. Log in to the console as configshell and select Security



2. Select Minimum Password Length
3. When prompted, enter configshell's password
4. Enter the new minimum password length



5. The change will take effect the next time a web or console user changes their password


Minimum Password Length
Minimum Password Length changed successfully
< OK >

10.4. Password Complexity

If this option is enabled using High Security Mode, all web and console user passwords must meet increased complexity requirements:

- Minimum length 8 characters
- Must use two of each
  - Upper case letters
  - Lower case letters
  - Numbers
  - Symbols
- No reusing previous password

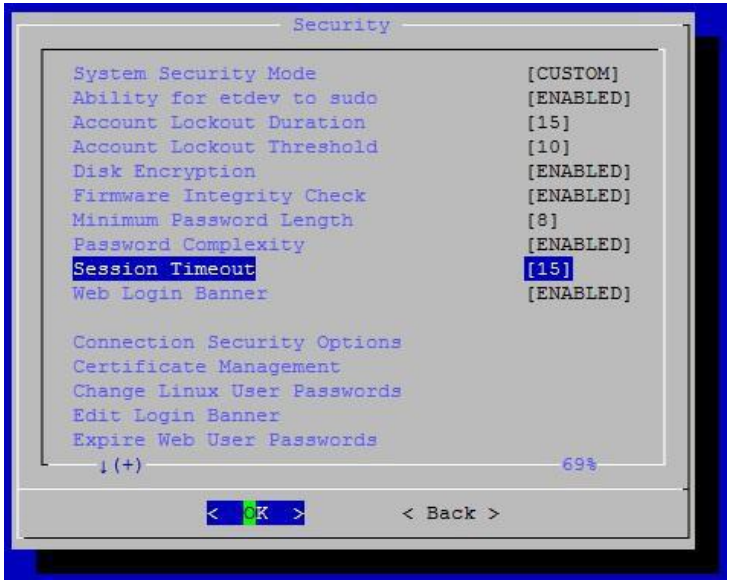
The allowed character list is:

- Upper case letters
- Lower case letters
- Numerals
- Special characters
- [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”]
- Other special characters:
- [“ “, “””, “‘”, “+”, ”,”, ”-”, ”.”, ”/”, ”:”, ”;”, ”<”, ”=”, ”>”, ”?”, ”[“, ”\”, ”]”, ”_”, ”`”, ”{“, ”|”, ”}”, ”~”]

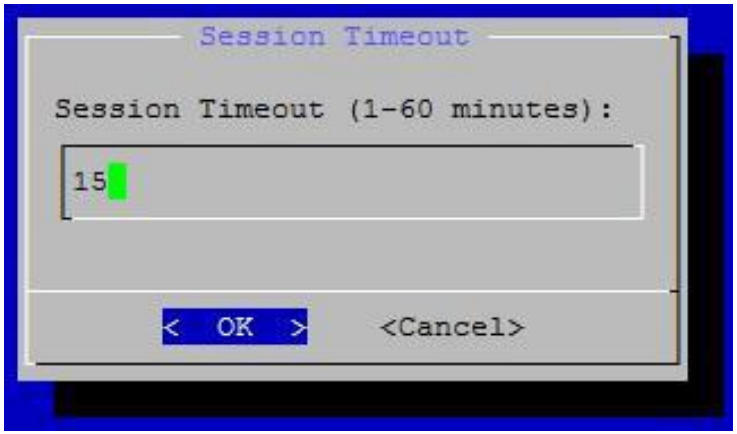
10.5. Session Timeout

Inactive console and web sessions are disconnected after a configurable session timeout.

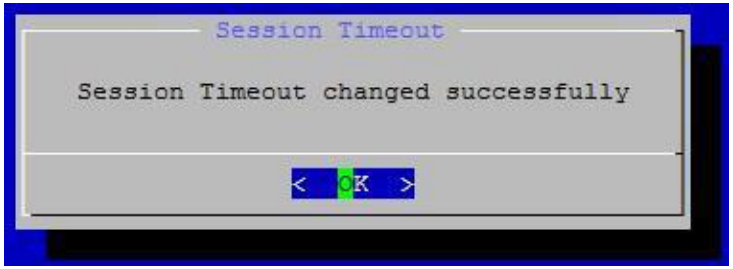
1. Log in to the console as configshell and select Security
2. Select Session Timeout



3. When prompted, enter configshell's password
4. Enter the new session timeout (in minutes)



5. The change will take effect for any new user logins



11. USER PASSWORD MANAGEMENT

11.1. Change Linux User Passwords

At any time, the Linux (or console) user passwords can be changed, subject to password complexity requirements depending on the current system security level. These passwords are forced to change when entering High Security Mode.

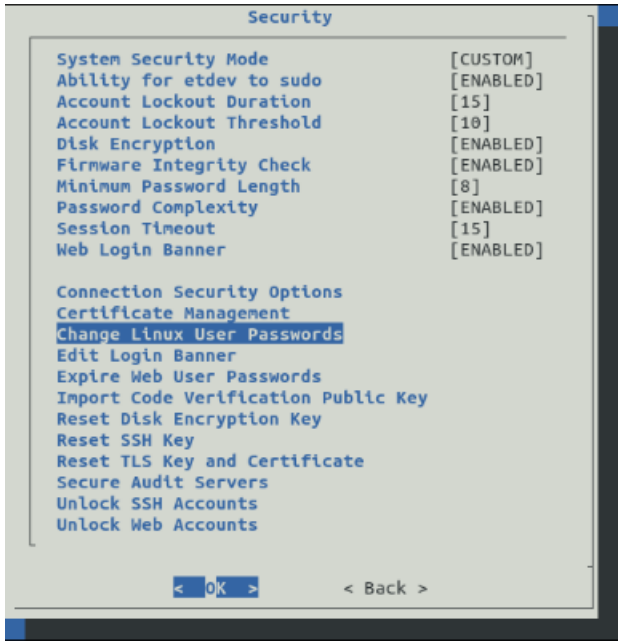
In High Security Mode, all web and console passwords must meet increased complexity requirements:

- Minimum length 8 characters
- Must use two of each
  - Upper case letters
  - Lower case letters
  - Numbers
  - Symbols
- No reusing previous password

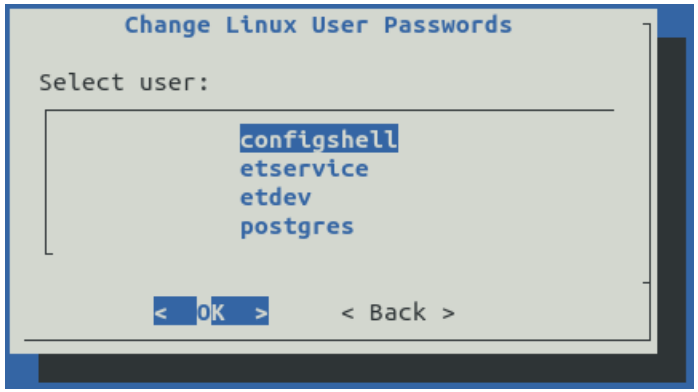
The allowed character list is:

- Upper case letters
- Lower case letters
- Numerals
- Special characters
- [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”]
- Other special characters:
- [“ “, “””, “‘”, “+”, ”,”, ”-”, ”.”, ”/”, ”:”, ”;”, ”<”, ”=”, ”>”, ”?”, ”[“, ”\”, ”]”, ”_”, ”`”, ”{“, ”|”, ”}”, ”~”]

1) Log in to the console as **configshell** and select **Security**
2) Select **Change Linux User Passwords**

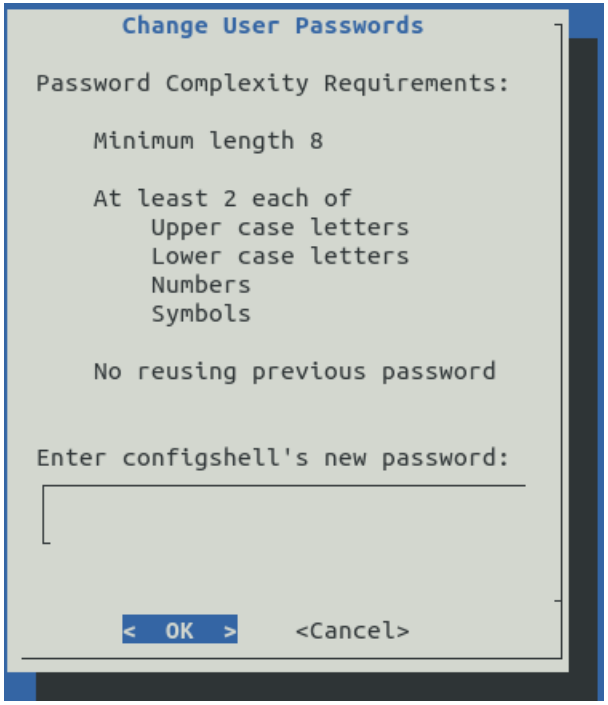


3) Select the target user (the postgres user is internal but also has a password)



4) When prompted, enter **configshell**'s password first, regardless of the target user

5) Enter the user's new password, twice for confirmation, adhering to the displayed password complexity requirements

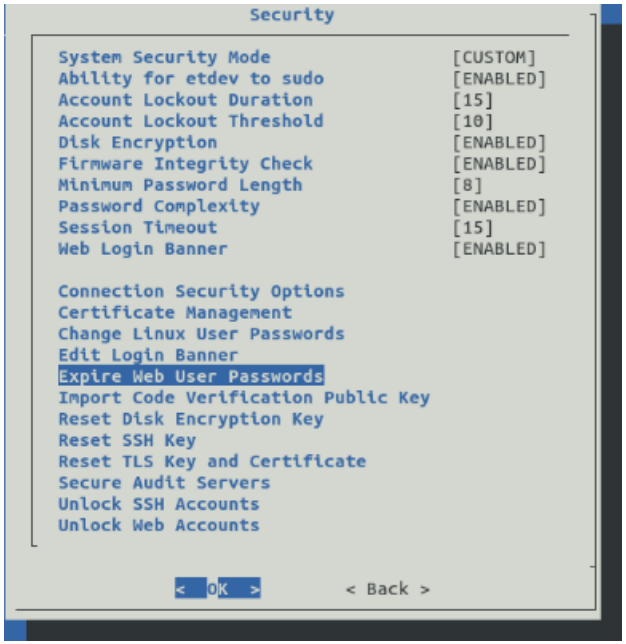


6) Repeat this process for other users as necessary

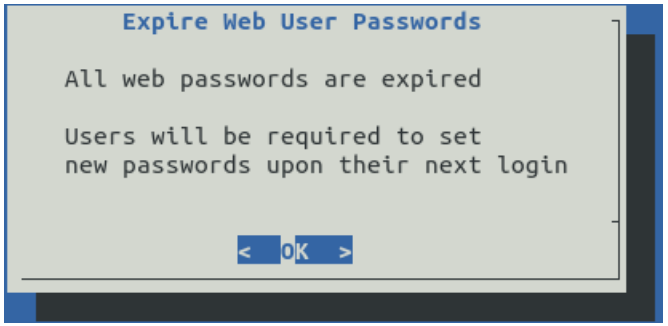
11.2. Expire Web User Passwords

A console administrator can force all web users (including admin) to change their password by expiring all of them simultaneously. Each user will be forced to change their password at their next successful login, subject to password complexity requirements. These same passwords are automatically expired when entering High Security Mode.

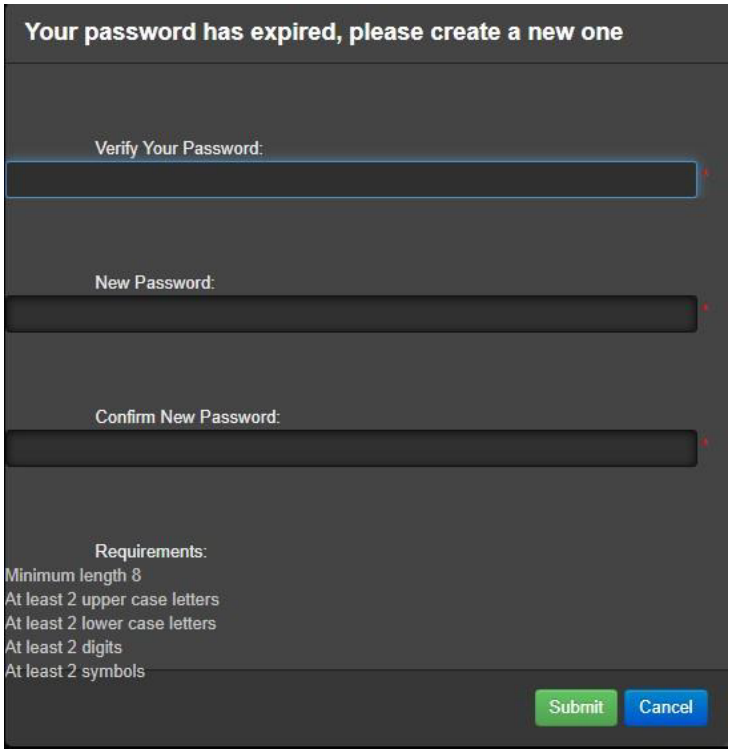
1) Log in to the console as configshell and select Security
2) Select Expire Web User Passwords



3) When prompted, enter configshell's password



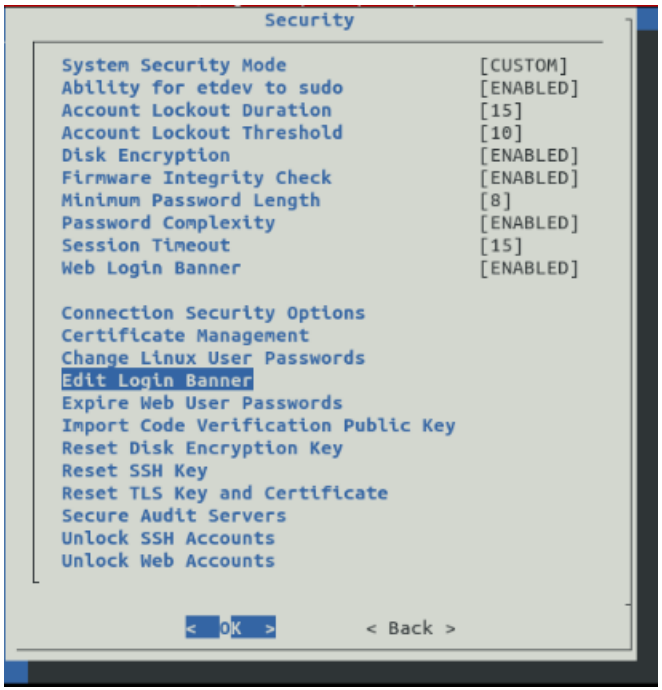
4) Each web user will be forced to change their password at their next login


Your password has expired, please create a new one
Verify Your Password:
New Password:
Confirm New Password:
Requirements:
Minimum length 8
At least 2 upper case letters
At least 2 lower case letters
At least 2 digits
At least 2 symbols
Submit
Cancel

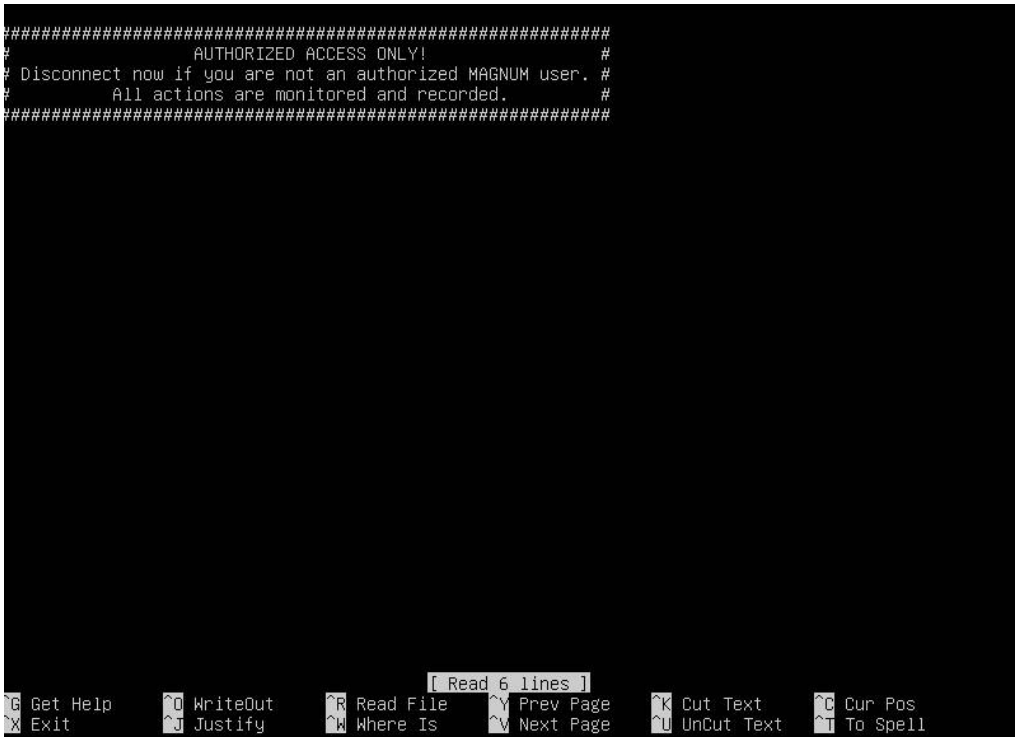
12. WEB LOGIN BANNER

The message in MAGNUM's login banner can be customized, depending on each organization's requirements. The console and web login banners share the same message.

1) Log in to the console as **configshell** and select **Security**
2) Select Edit Login Banner

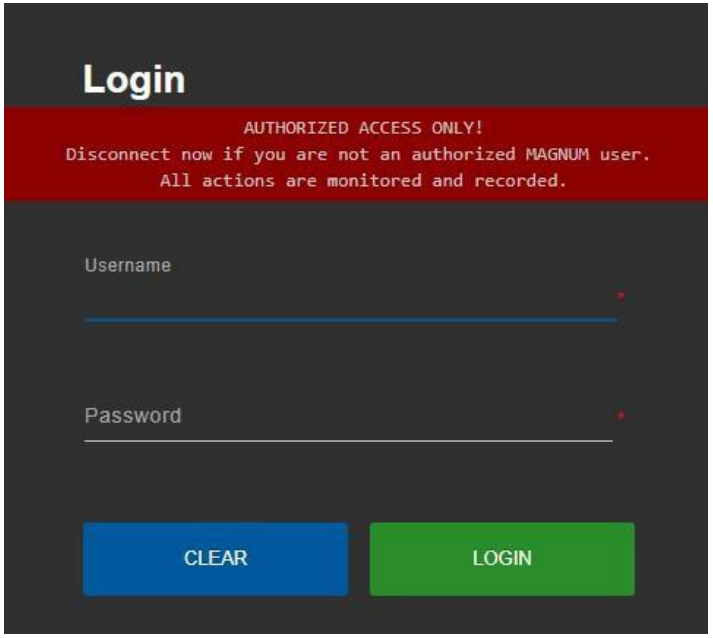


3) Edit the message as required. The editor is called "nano" (see https://www.nanoeditor.org/docs.php for details on how to use)



4) To save and exit press **<CTRL>X**, then **Y**, then **<Enter>**

If the login banner option is enabled, web users will see a red warning banner before entering their credentials:



13. CERTIFICATE MANAGEMENT

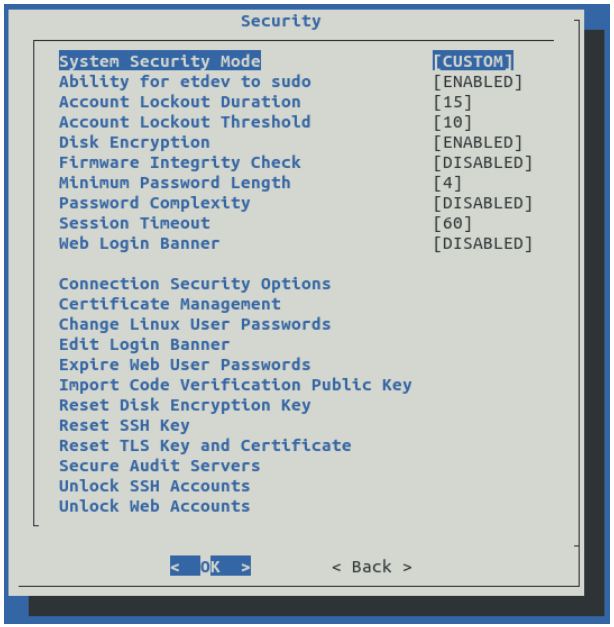
Note:

1. *X.509 certificates are used to authenticate all TLS connections. A client certificate is sent whenever the server requests one. This functionality cannot be disabled.*
2. *Only certificates in PEM format are supported (DER is not supported).*
3. *Certificate Revocation Lists (CRLs) are downloaded from CRL-DP extensions during each connection attempt, if the peer certificates define them (only for end-user and intermediate certificates, not for root CA certificates).*
4. *Recommend removing the Evertz default CA and CRL during system setup, to replace them with organization-specific certificates.*

13.1. Show Server Certificate

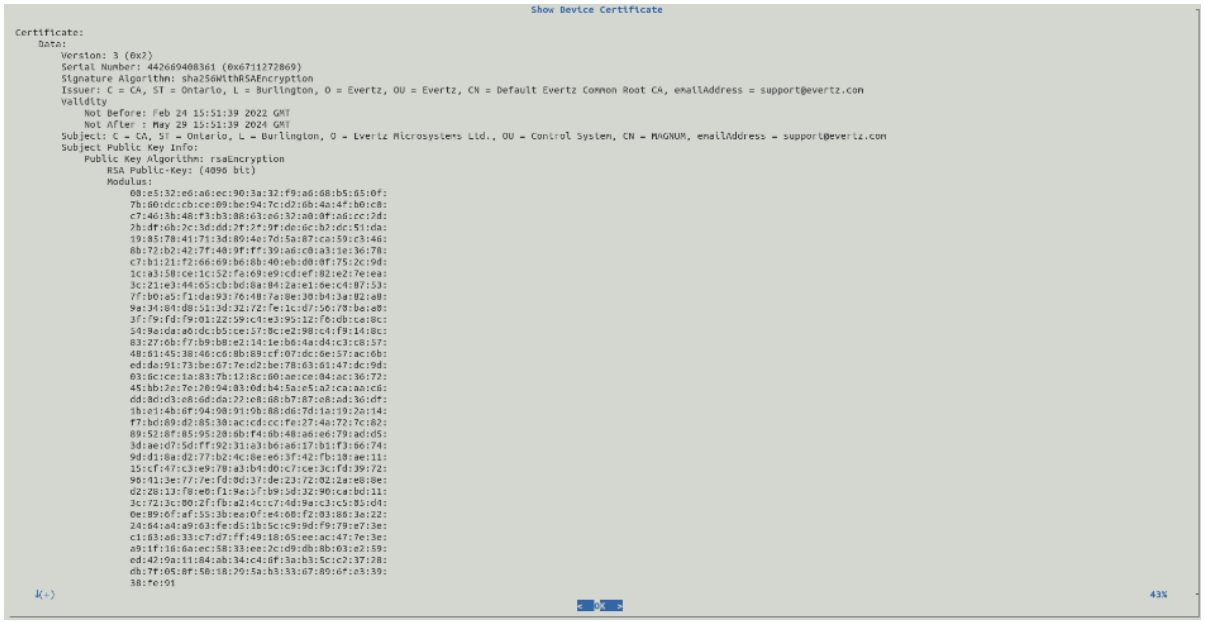
This option allows the administrator to review the certificate that identifies the MAGNUM device

1. Log in to the console as configshell and select Security



2. Select Certificate Management

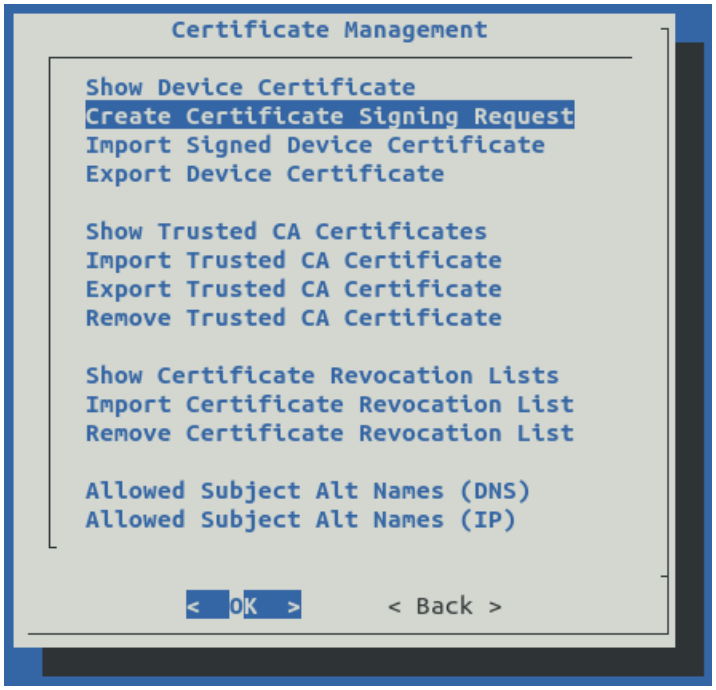
3. Select Show Server Certificate
4. Review the certificate details, using the arrow keys to scroll down or right



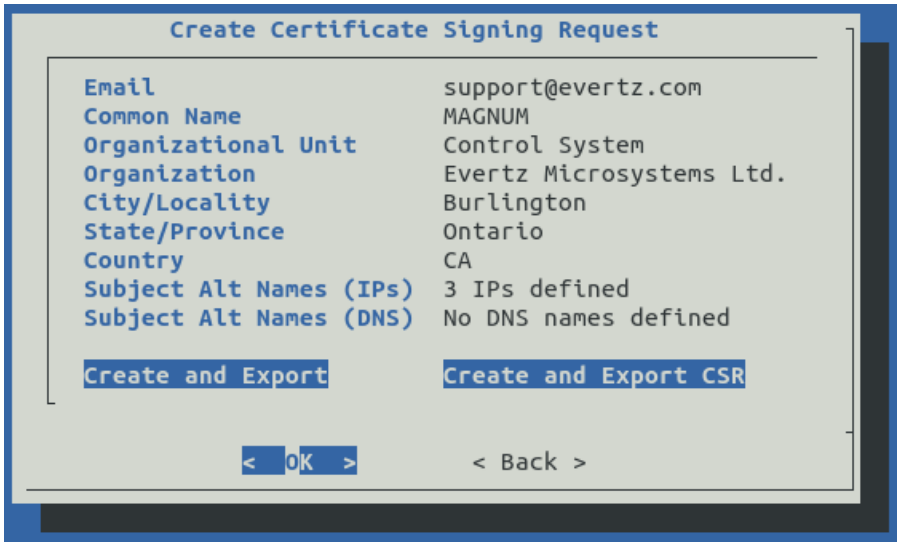
13.2. Create Certificate Signing Request

MAGNUM initially powers on with a certificate signed by the default Evertz CA. It is recommended to replace this with organization-specific certificates, where a CSR is generated and signed by the organization's CA. This option allows an administrator to create and export a CSR. It is derived from the device's TLS key, which is unique to each device and automatically generated at first power-on, when entering High Security Mode, or when manually reset. The CSR is created with editable fields, but it is expected that the organization's CA will provide its own when creating a signed certificate for the device. The CSR will automatically include the device's current IP addresses in the SAN field.

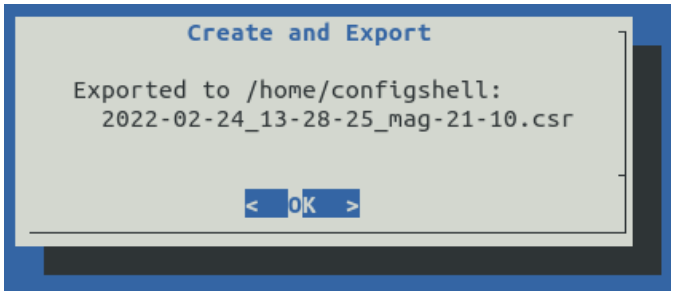
1. Log in to the console as configshell and select Security
2. Select Certificate Management
3. Select Create Certificate Signing Request



4. Update each field as appropriate for the particular device and organization



5. Select Create and Export
6. Select the destination, either /home/configshell via SFTP or USB Device
7. The file name is auto-generated during export

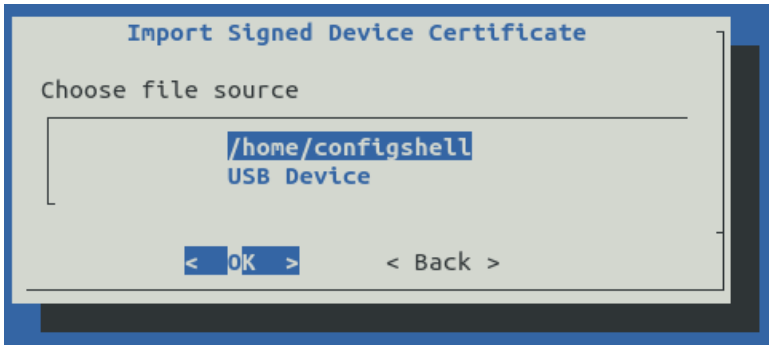


13.3. Import Signed Device Certificate

After the organization's CA signs a previously exported CSR to create a signed certificate, this option allows the administrator to import the certificate into MAGNUM. This certificate will identify the MAGNUM device to the other devices to which it connects

1. Log in to the console as configshell and select Security
2. Select Certificate Management
3. Select Import Signed Server Certificate

4. When prompted, enter configshell's password
5. Select the file's source, either /home/configshell via SFTP or USB Device
6. Select the correct certificate file (must be in PEM format with a .pem extension)

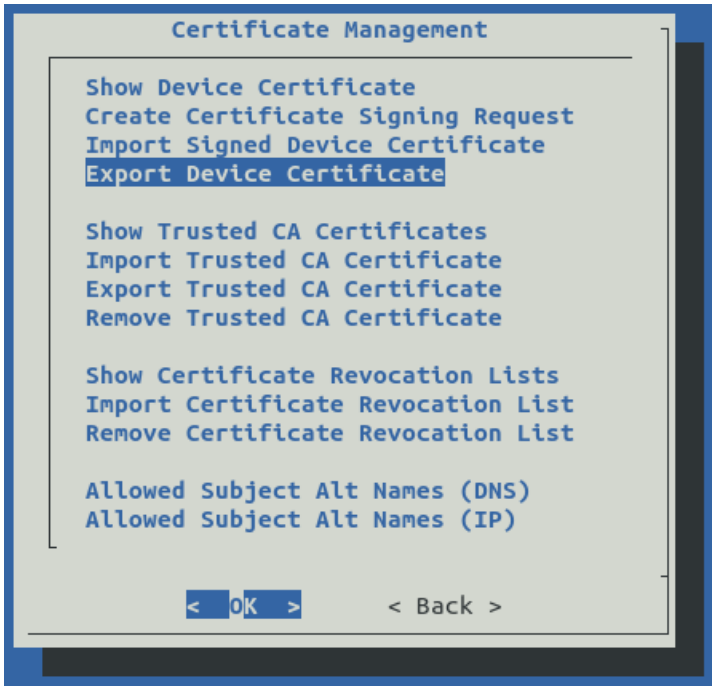


7. When prompted, reboot

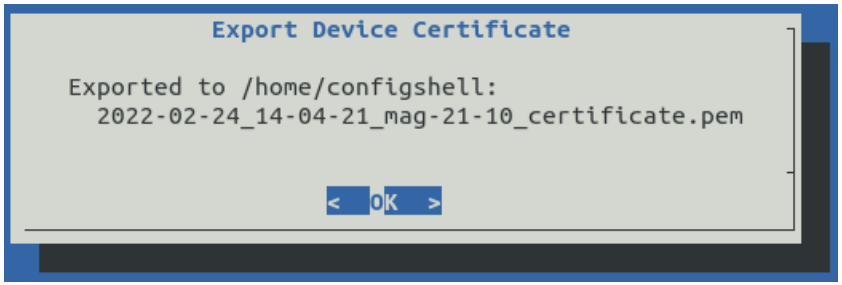
13.4. Export Server Certificate

Export the MAGNUM device's certificate used for all TLS connections, if a need for that arises. This only includes the device's public key, not the private key.

1. Log in to the console as **configshell** and select **Security**
2. Select Certificate Management
3. Select Export Server Certificate



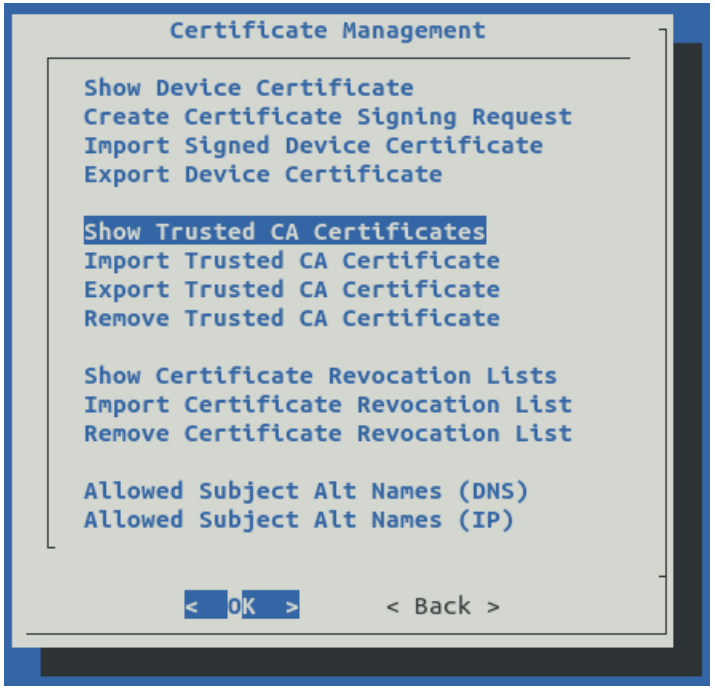
4. When prompted, enter **configshell**'s password
5. Select the file's source, either /home/configshell via SFTP or USB Device
6. The file name is auto-generated during export



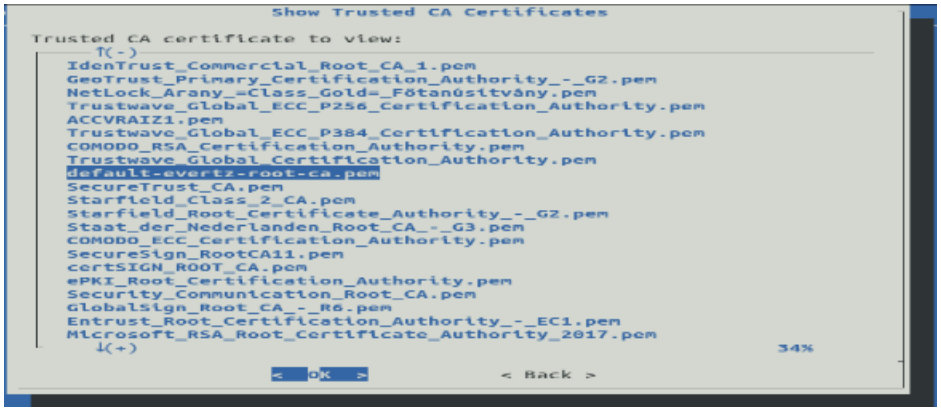
13.5. Show Trusted CA Certificates

This option allows the administrator to review the CA certificates trusted by a MAGNUM device. This option is useful before and after importing or removing trusted CA certificates. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. They must all be signed by a trusted CA. Each CA in the chain must be explicitly imported from here to be trusted.

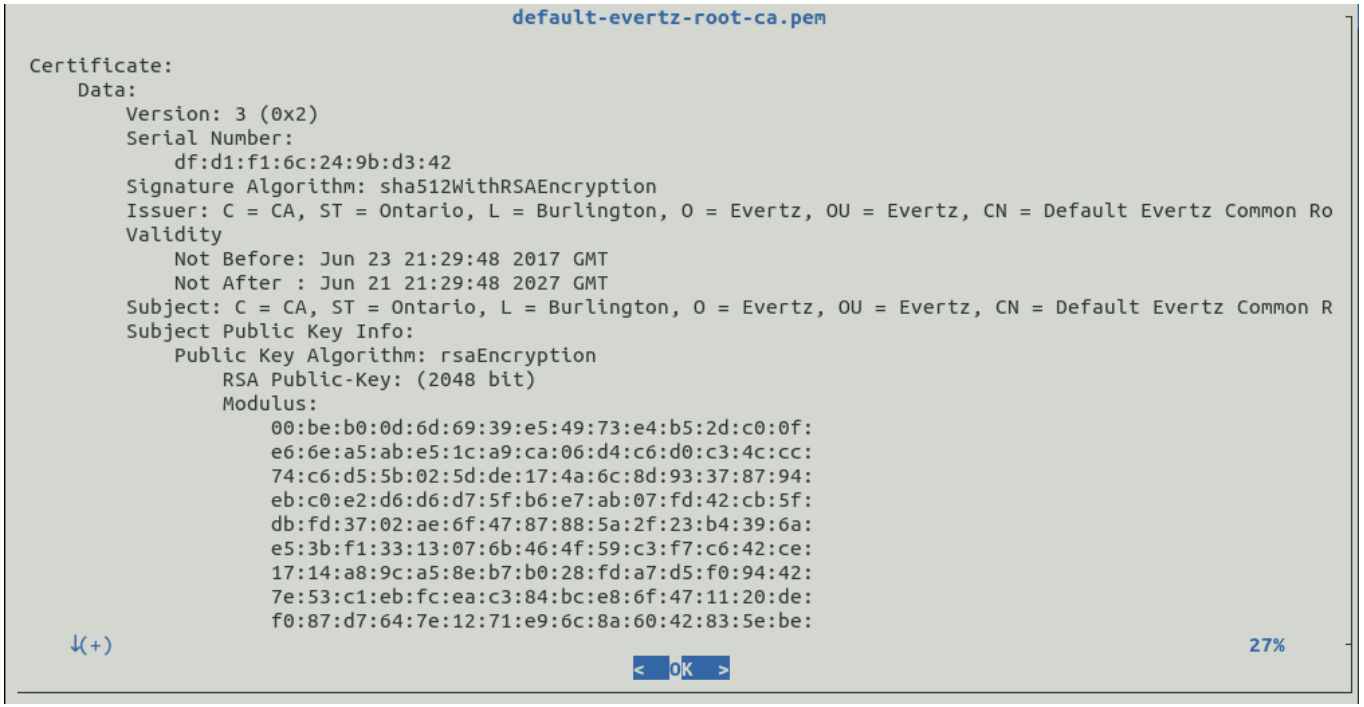
1. Log in to the console as **configshell** and select **Security**
2. Select Certificate Management
3. Select **Show Trusted CA Certificates**



4. Select a particular CA certificate to review



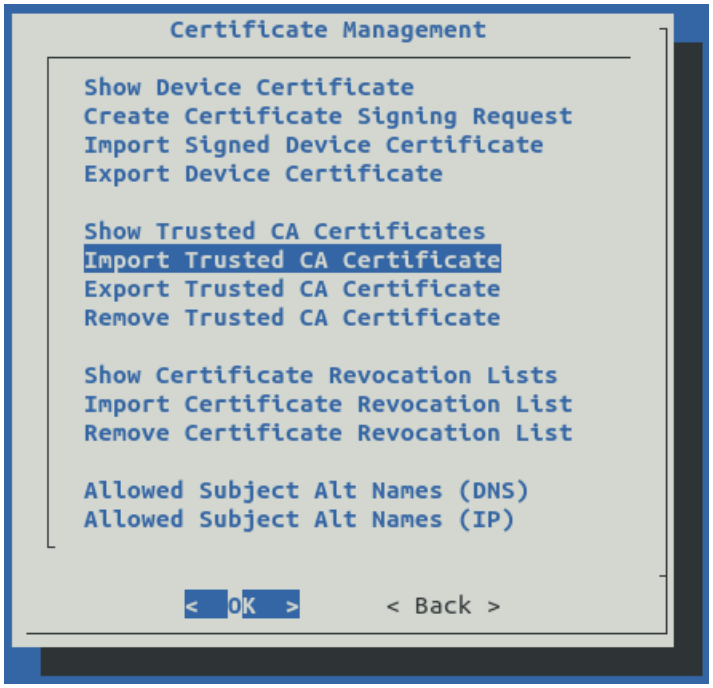
5. Review the certificate details, using the arrow keys to scroll down or right



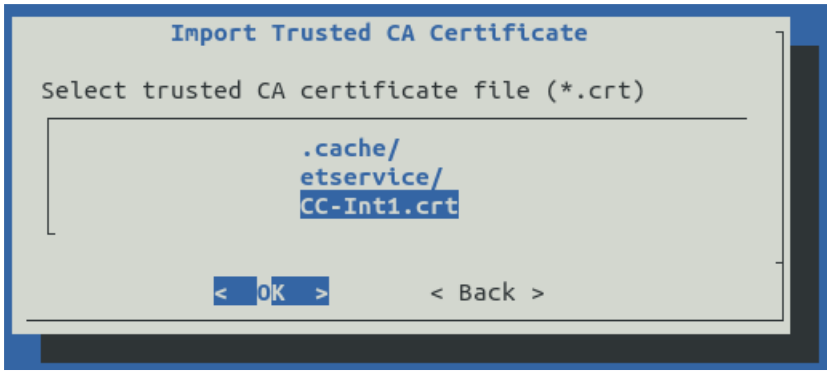
13.6. Import Trusted CA Certificate

Import and thereby trust a CA certificate. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. They must all be signed by a trusted intermediate or root CA. Each CA in the chain must be explicitly imported from here to be trusted.

1. Log in to the console as **configshell** and select **Security**
2. Select Certificate Management
3. Select Import Trusted CA Certificate



4. When prompted, enter **configshell**'s password
5. Select the file's source, either /home/configshell via SFTP or USB Device
6. Select the correct CA certificate file (must be in PEM format with a .crt extension)

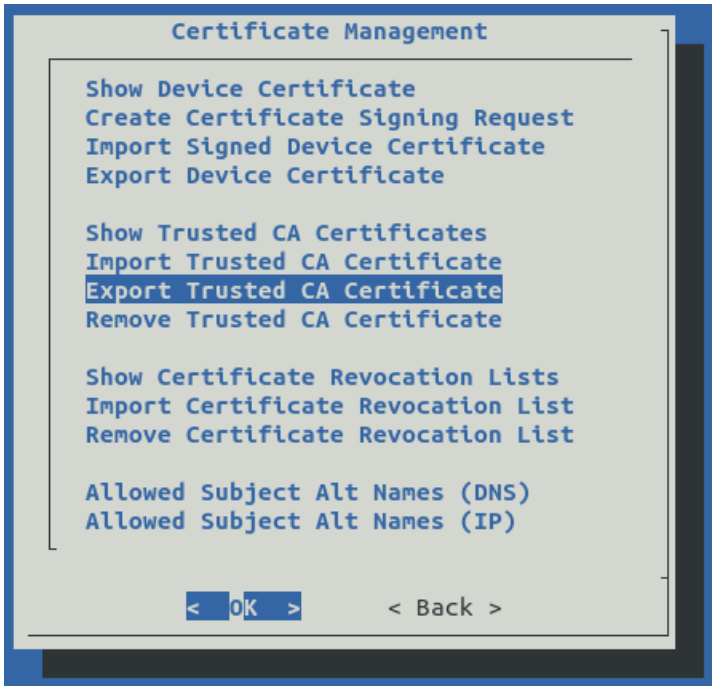


7. After the CA certificate is imported, the changes will take place immediately

13.7. Export Trusted CA Certificate

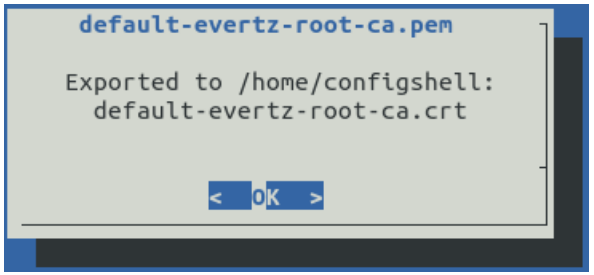
Export any trusted CA certificate, if a need for that arises.

1. Log in to the console as **configshell** and select **Security**
2. Select **Certificate Management**
3. Select **Export Trusted CA Certificate**



4. When prompted, enter **configshell's** password
5. Select the CA certificate to export

6. Select the file's source, either /home/configshell via SFTP or USB Device
7. The file name is kept the same after export

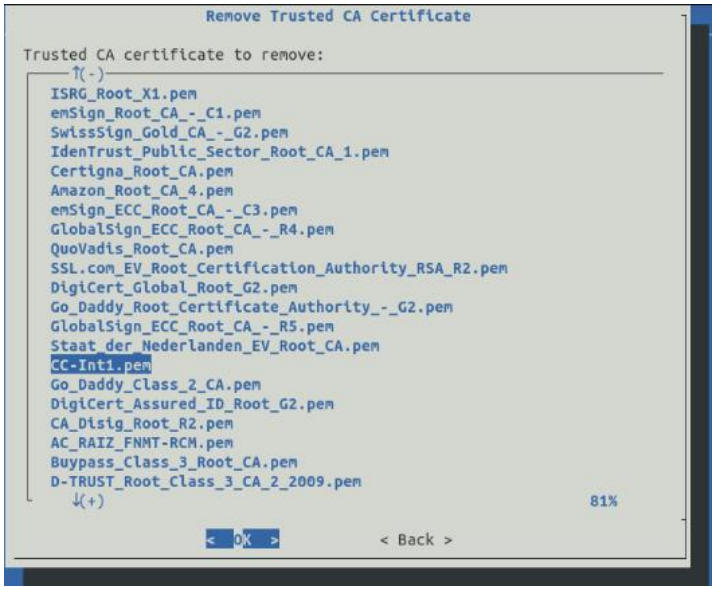


13.8. Remove Trusted CA Certificate

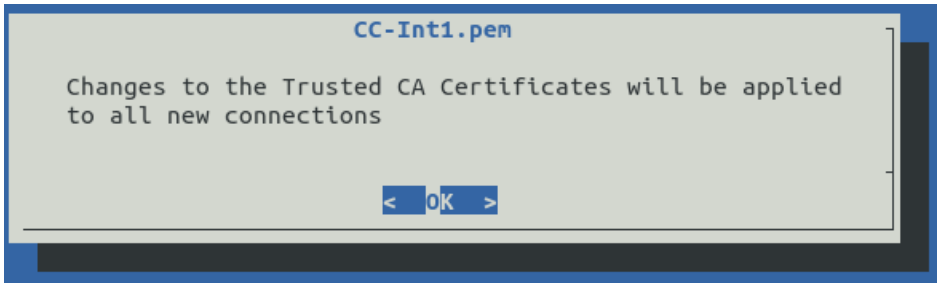
Remove and thereby stop trusting a CA certificate. In High Security Mode, all CA certificates must have a corresponding CRL, which must be removed first. This is enforced by MAGNUM to ensure there are no stale CRLs.

1. Log in to the console as **configshell** and select **Security**
2. Select **Certificate Management**
3. Select Remove Trusted CA Certificate

4. Select the trusted CA certificate to remove and stop trusting



5. When prompted, enter **configshell**'s password
6. The change will take effect for all new TLS connections

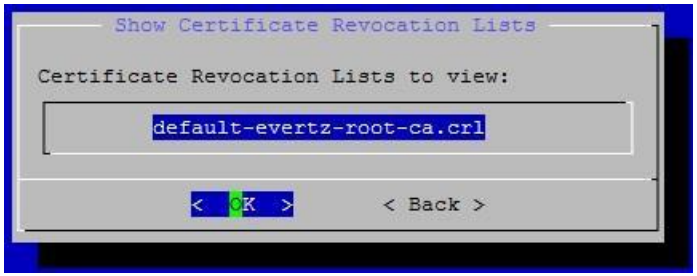


13.9. Show Certificate Revocation List

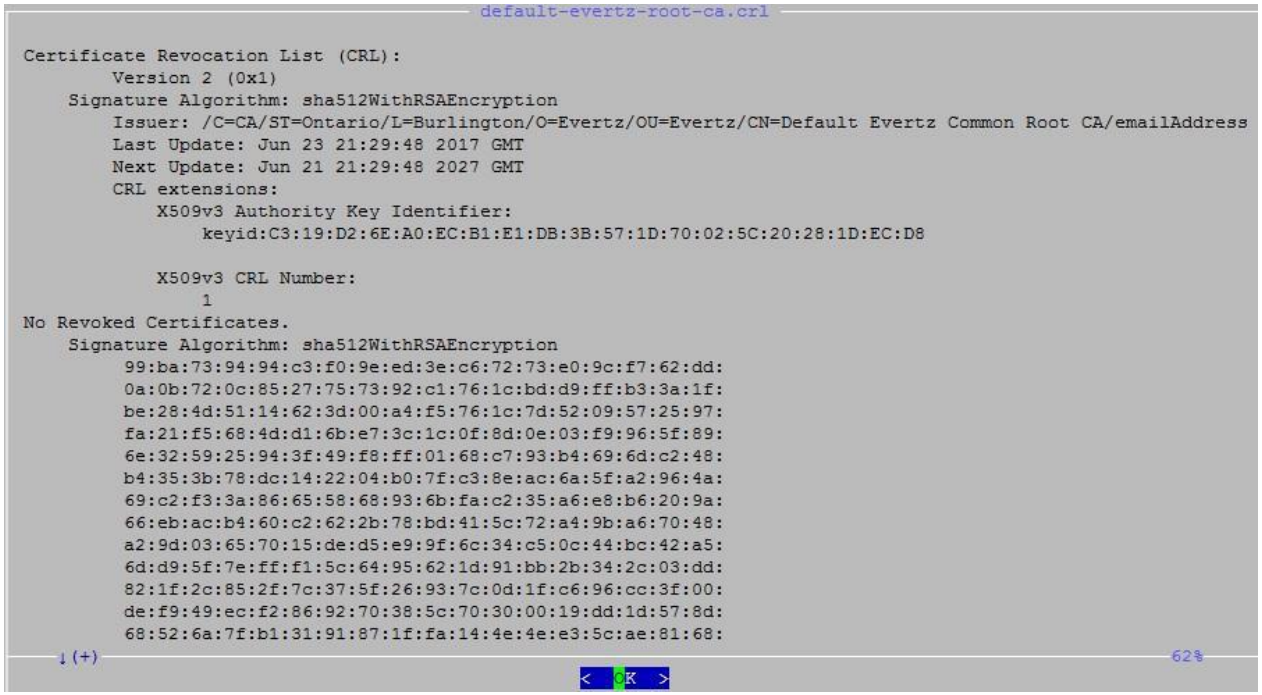
This option allows the administrator to review CRLs. This option is useful before and after importing or removing CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first

1) Log in to the console as configshell and select Security
2) Select Certificate Management
3) Select Show Certificate Revocation List

4) Select the CRL to review



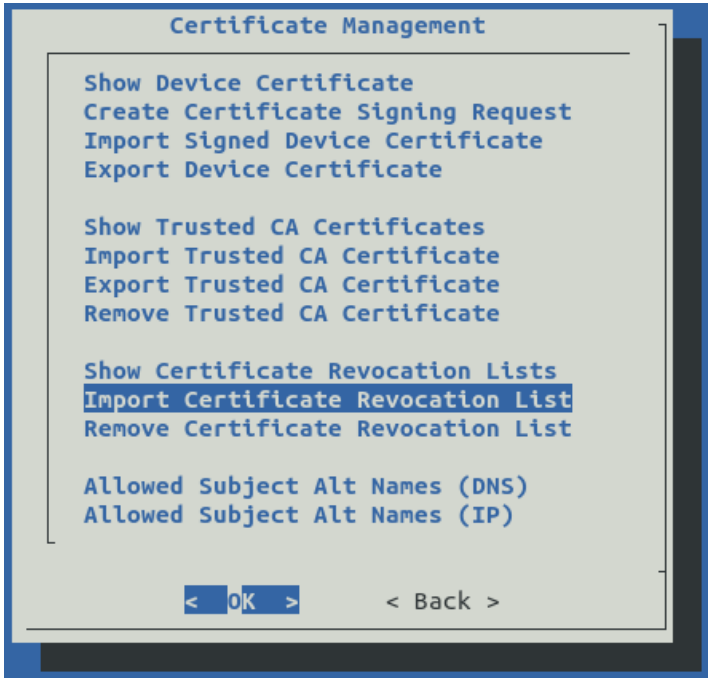
5) Review the CRL details, using the arrow keys to scroll down or right



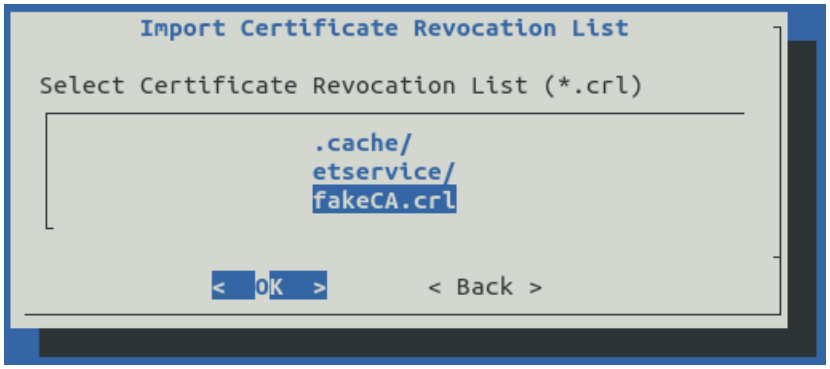
13.10. Import Certificate Revocation List

This option allows the administrator to import CRLs. In High Security Mode, all TLS connections are authenticated by verifying the peer's certificate. If peer's certificate is revoked by an imported CRL, the connection is blocked. Every trusted CA certificate must have a corresponding CRL. The CAs must be imported first. If the peer's end-entity or intermediate CA certificates include a CRL-DP extension, it will be downloaded at every connection attempt, and the connection will be denied if either the download fails or the downloaded CRL revokes a certificate along the peer's certificate chain.

1) Log in to the console as configshell and select Security
2) Select Certificate Management
3) Select Import Certificate Revocation list



4) When prompted, enter configshell's password
5) Select the file's source, either /home/configshell via SFTP or USB Device
6) Select the correct CRL file (must have a .crl extension)



7) The change will take effect for all new TLS connections

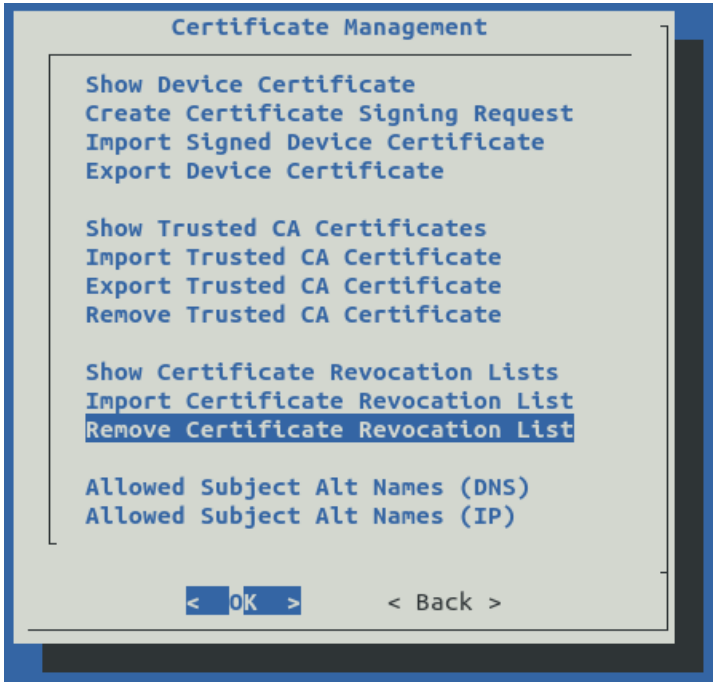
13.11. Remove Certificate Revocation List

This option allows the administrator to remove and thereby stop checking a CRL. Until the corresponding CA certificate is also removed, MAGNUM will not establish new TLS connections, because in High Security Mode, all CA certificates must have a corresponding CRL.

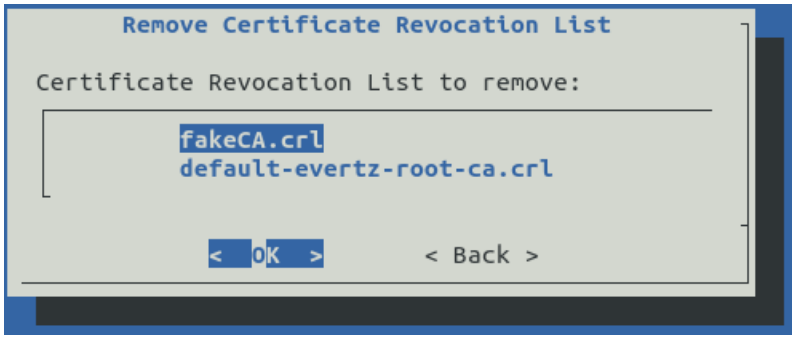
1) Log in to the console as configshell and select Security

2) Select Certificate Management

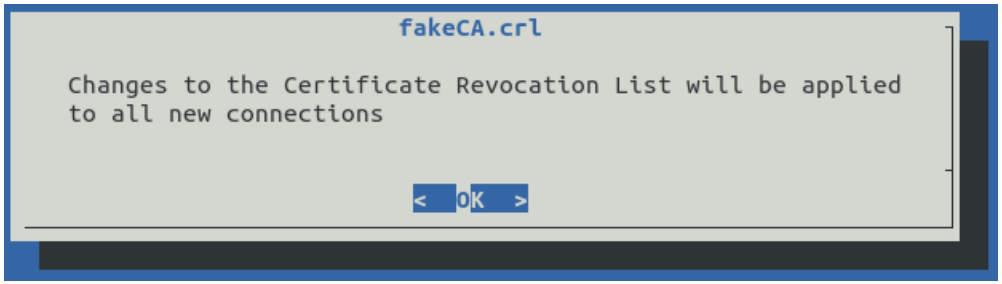
3) Select Remove Certificate Revocation List



4) Select the CRL to remove



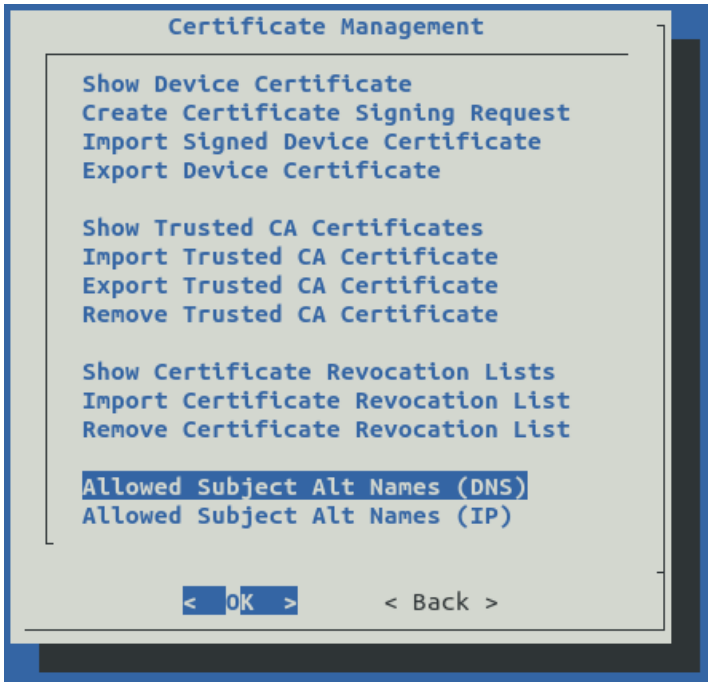
5) When prompted, enter configshell's password
6) The change will take effect for all new TLS connections



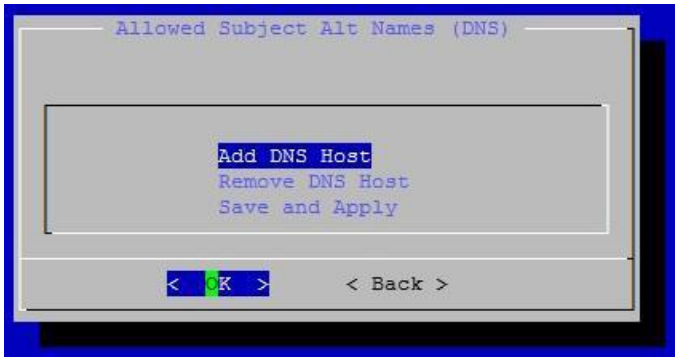
13.12. Allowed Subject Alt Names (DNS)

This option allows the administrator to configure a list of allowed Subject Alternative Names (also known as reference identifiers). In High Security Mode, all TLS connections (including both client and server connections) are authenticated by verifying the peer's certificate. If the peer's certificate does not contain a Subject Alternative Name field from the MAGNUM device's allowed list, the connection is blocked. If the allowed list is empty, this field is not checked during certificate authentication. If the peer's certificate does not have a Subject Alternative Names field, the Common Name field is checked instead, for backwards compatibility.

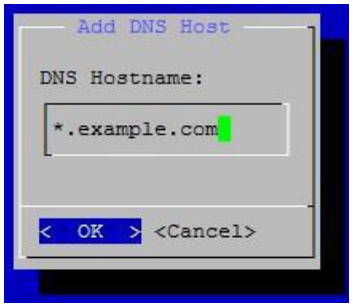
1) Log in to the console as **configshell** and select **Security**
2) Select Certificate Management
3) Select Allowed Subject Alt Names (DNS)



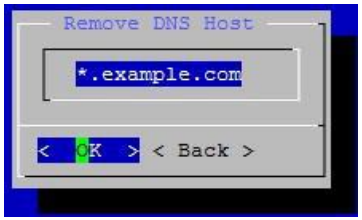
4) Select **Add DNS Host** to add new entries



5) Enter a valid DNS name (wildcards are supported)



6) Select **Remove DNS Host** to remove entries



7) Select **Save and Apply** when done

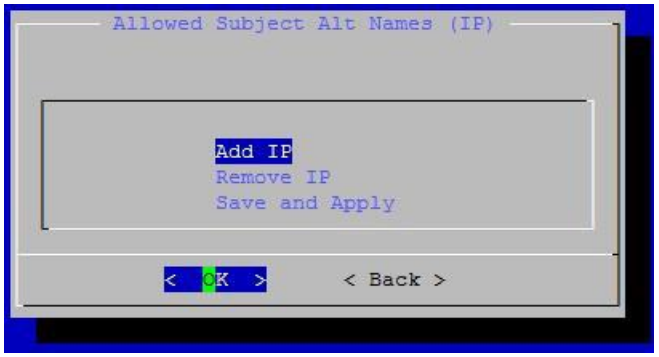
8) When prompted, reboot

13.13. Allow Subject Alt Names (IP)

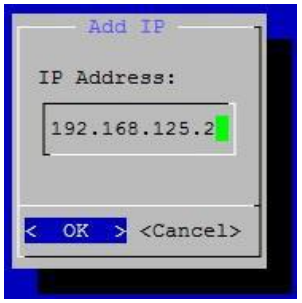
This option allows the administrator to configure a list of allowed Subject Alternative Names (also known as reference identifiers). In High Security Mode, all TLS connections (including both client and server connections) are authenticated by verifying the peer's certificate. If the peer's certificate does not contain a Subject Alternative Name field from the MAGNUM device's allowed list, the connection is blocked. If the allowed list is empty, this field is not checked during certificate authentication.

1) Log in to the console as configshell and select Security
2) Select Certificate Management
3) Select Allowed Subject Alt Names (IP)

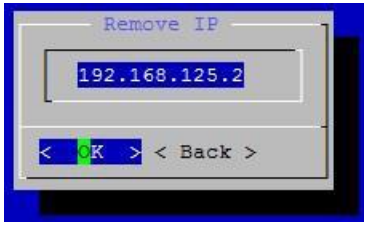
4) Select **Add IP** to add new entries



5) Enter a valid IP address



6) Select **Remove IP** to remove entries



7) Select **Save and Apply** when done

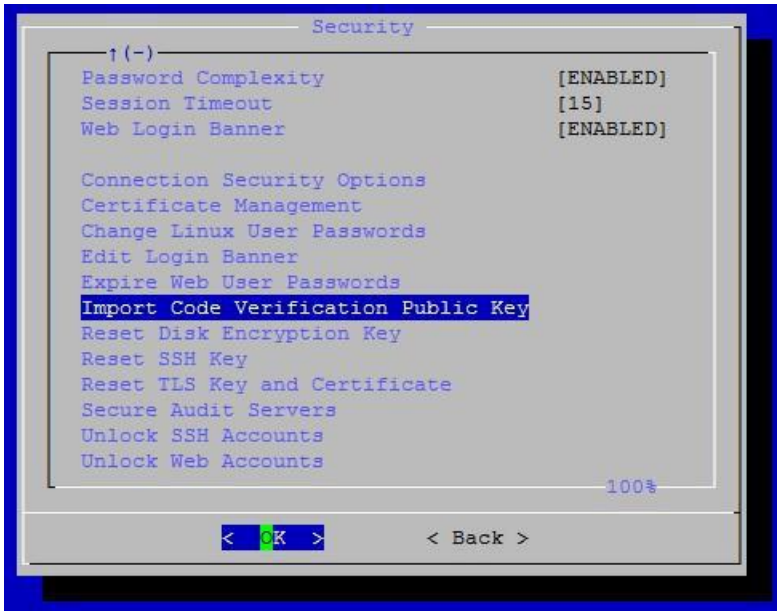
8) When prompted, reboot

13.14. Cryptographic Key Management

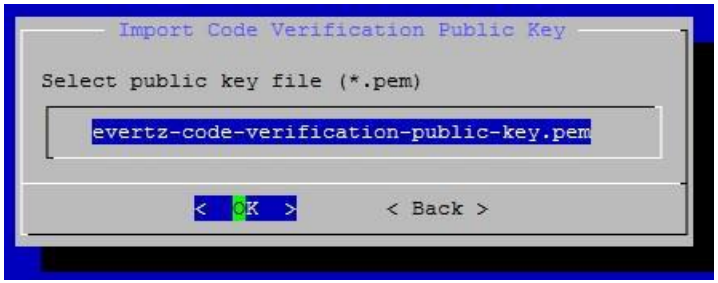
13.15. Import Code Verification Public Key

In High Security Mode, all firmware upgrade images (.efp files) will have their signatures (.sig files) verified before being installed. Evertz signs these firmware images at build-time, and this menu option provides the ability to change the code verification public key, allowing upgrades to continue if Evertz changes its private signing key.

1. Log in to the console as configshell and select Security
2. Select Import Code Verification Public Key



3. Select the file's source, either /home/configshell via SFTP or USB Device
4. Select the public key to import

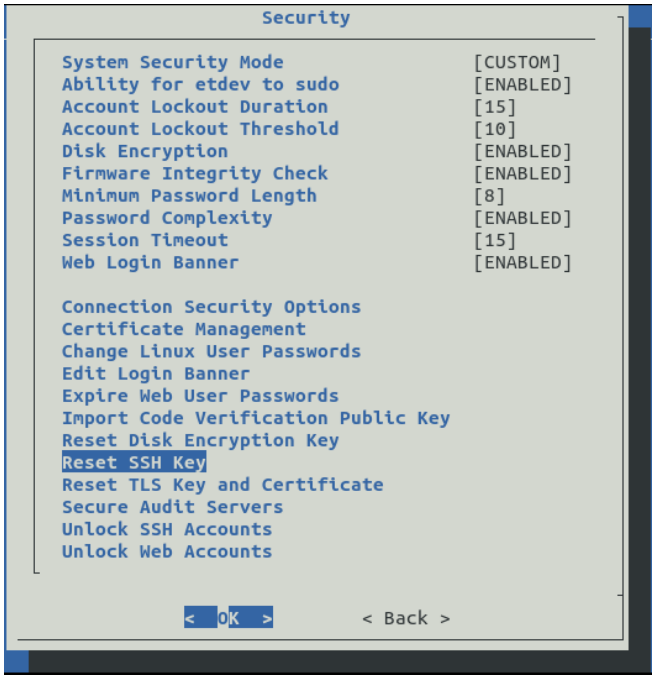


5. The change will take effect immediately

13.16. Reset SSH Key

Erase the device's current SSH Key and generate a new one during reboot.

1. Log in to the console as **configshell** and select **Security**
2. Select Reset SSH Key



3. Select Yes to proceed

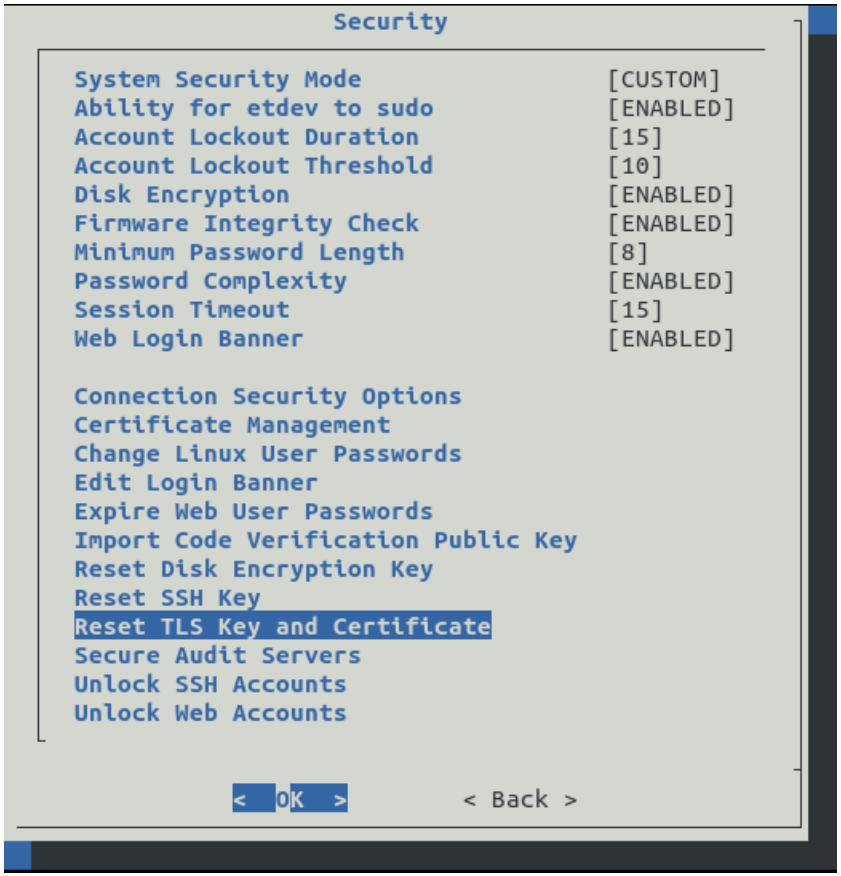
4. When prompted, enter **configshell**'s password
5. When prompted, reboot

6. A new key will be automatically generated during power-on. If the device does not have a graceful shutdown, the key may not be zeroized and the process should be repeated.

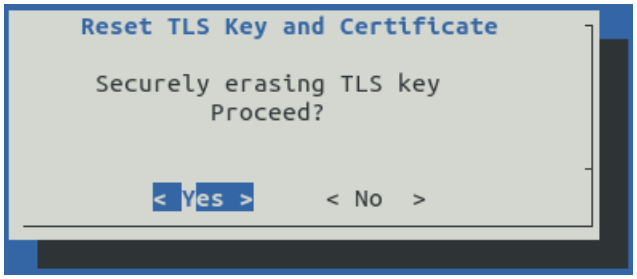
13.17. Reset TLS Key and Certificate

In High Security Mode, MAGNUM encrypts all TLS connections with TLSv1.2. This option allows an administrator to change the private TLS key at any time. The new random key is chosen automatically. A new self-signed certificate will also be created, replacing any existing certificate identifying the device. The administrator should generate a new CSR and have it signed by a CA before MAGNUM reconnects to other devices.

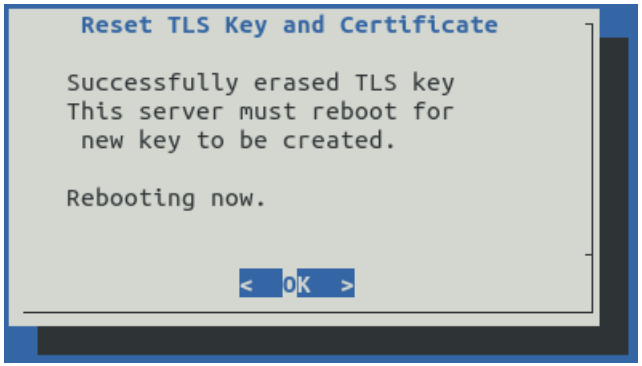
1. Log in to the console as configshell and select Security
2. Select Reset TLS Key and Certificate



3. Select Yes to proceed



4. When prompted, enter configshell's password
5. When prompted, reboot



6. A new key and self-signed certificate are automatically generated during power-on. If the device does not have a graceful shutdown, the key may not be zeroized and the process should be repeated.
7. Create a new CSR, sign it, and import it before connecting MAGNUM to other devices

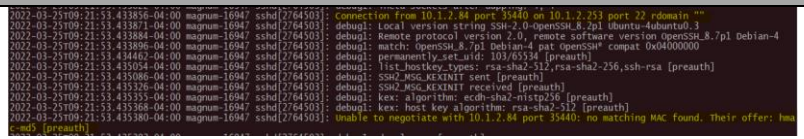
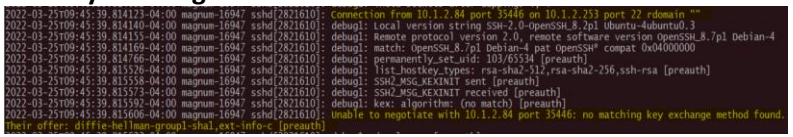
14. AUDIT LOGS AND SYSLOG CONFIGURATION

14.1. Auditable Events

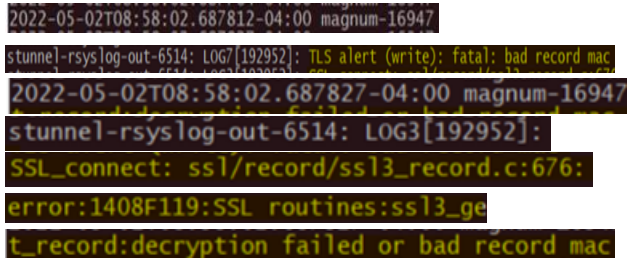
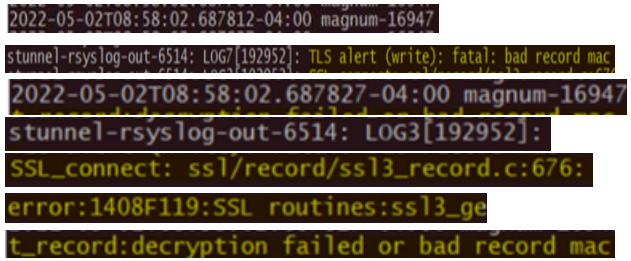
When the audit events in the system are full the TOE will drop new audit messages. If this highly unlikely event occurs, the administrators will have to manually clear the unnecessary files by login in to the shell as the 'configshell' user to make space or increase the disk space by attaching a new hard disk.

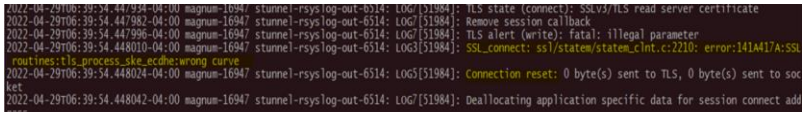
The following table reflects the list of auditable events that the Magnum hardware record:

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session	Reason for failure	Please refer to 'FCS_TLSS_EXT.1 failures below
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	**Bad Credentials:** 2022-03-24T06:57:18.972435-04:00 magnum-16947 sshd[3171244]: debug1: PAM: password authentication failed for etdev: Authentication failure 2022-03-24T06:57:18.972492-04:00 magnum-16947 sshd[3171244]: Failed password for etdev from 10.1.2.84 port 35368 ssh2 **Bad packet length:** 2022-10-31T05:33:22.289924-04:00 magnum-86432 sshd[1367533]: Bad packet length 3500028. 2022-10-31T05:33:22.289986-04:00 magnum-86432 sshd[1367533]: ssh_dispatch_run_fatal: Connection from user etdev 10.1.2.84 port 48282: message authentication code incorrect **Bad integrity algorithm:**

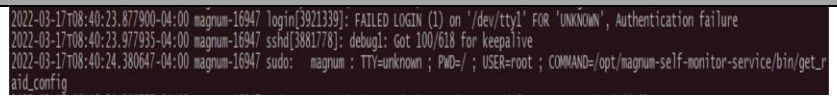
Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			 **Bad key exchange:** 
FCS_TLSC_EXT.1	Failure to establish a TLS session	None	2022-07-13T10:25:10.647137-04:00 magnum-86432 stunnel-rsyslog-out- 6514: LOG3[2123]: SSL_connect: ssl/statem/statem_clnt.c:1913: error:1416F086:SSL routines:tls_process_server_certificate: certificate verify failed **Bad Cert Type:** 2022-10-27T12:36:19.252716-04:00 magnum-86432 stunnel-rsyslog-out- 6514: LOG7[2973]: TLS alert (write): fatal: illegal parameter 2022-10-27T12:36:19.252990-04:00 magnum-86432 stunnel-rsyslog-out- 6514: LOG3[2973]: SSL_connect: ssl/statem/statem_clnt.c:1957: error:1416F17F:SSL routines:tls_process_server_certificate:wrong certificate type **Bad Ciphersuite:** 2022-04-28T07:55:53.810365-04:00 magnum-16947 stunnel-

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			rsyslog-out-6514: LOG7[8779]: TLS alert (write): fatal: illegal parameter 2022-04-28T07:55:53.810376-04:00 magnum-16947 stunnel-rsyslog-out-6514: LOG3[8779]: SSL_connect: ssl/statem/statem_clnt.c:1333: error:1421C0F8:SSL routines:set_client_ciphersuite:unknown cipher returned **Bad Protocol Version:** 2022-04-29T07:54:52.693264-04:00 magnum-16947 stunnel-rsyslog-out- 6514: LOG7[54350]: TLS alert (write): fatal: protocol version 2022-04-29T07:54:52.693279-04:00 magnum-16947 stunnel-rsyslog-out- 6514: LOG3[54350]: SSL_connect: ssl/statem/statem_lib.c:1957: error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol **Bad Signature Verification:** 2022-04-29T08:10:53.751345-04:00 magnum-16947 stunnel-rsyslog-out- 6514: LOG7[54852]: TLS alert (write): fatal: decrypt error 2022-04-29T08:10:53.751360-04:00 magnum-16947 stunnel-rsyslog-out- 6514: LOG3[54852]: error queue: ssl/statem/statem_clnt.c:2406: error:1416D07B:SSL routines:tls_process_key_exchange:bad signature **Bad Decryption:**

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			 **Bad MAC:**  **Bad Certificate:** 2022-07-13T10:25:10.647125-04:00 magnum-86432 stunnel-rsyslog-out- 6514: LOG7[2123]: TLS alert (write): fatal: internal error 2022-07-13T10:25:10.647137-04:00 magnum-86432 stunnel-rsyslog-out- 6514: LOG3[2123]: SSL_connect: ssl/statem/statem_clnt.c:1913: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			Bad Negotiated Elliptic Curve: 
FCS_TLSS_EXT.1	Failure to establish a TLS Session	Reason for failure	2022-07-06T08:58:06.259800-04:00 magnum-86432 stunnel-nginx-in-443: LOG7[32]: TLS alert (write): fatal: handshake failure 2022-07-06T08:58:06.259812-04:00 magnum-86432 stunnel-nginx-in-443: LOG3[32]: SSL_accept: ssl/statem/statem_srvr.c:2283: error:1417A0C1: SSL routines:tls_post_process_client_hello:no shared cipher 2022-07-06T08:58:06.259838-04:00 magnum-86432 stunnel-nginx-in-443: LOG5[32]: Connection reset: 0 byte(s) sent to TLS, 0 byte(s) sent to socket **Decrypt Error:** 2022-07-06T07:24:07.031510-04:00 magnum-86432 stunnel-nginx-in-443: LOG7[21]: TLS alert (write): fatal: decrypt error 2022-07-06T07:24:07.031527-04:00 magnum-86432 stunnel-nginx-in-443: LOG3[21]: SSL_accept: ssl/statem/statem_lib.c:811: error:1416C095:SSL routines:tls_process_finished:digest check failed **Bad Protocol Version:** 2022-11-02T06:29:15.549275-04:00 magnum-86432 stunnel-nginx-in-443: LOG7[523]: TLS alert (write): fatal: protocol version 2022-11-02T06:29:15.549287-04:00 magnum-86432 stunnel-nginx-in-443: LOG3[523]: SSL_accept: ssl/statem/statem_srvr.c:1659: error:142090FC:SSL routines:tls_early_post_process_client_hello:

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			unknown protocol **Unsupported EC Curve:** 2022-07-06T08:58:06.259800-04:00 magnum-86432 stunnel-nginx-in-443: LOG7[32]: TLS alert (write): fatal: handshake failure 2022-07-06T08:58:06.259812-04:00 magnum-86432 stunnel-nginx-in-443: LOG3[32]: SSL_accept: ssl/statem/statem_srvr.c:2283: 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)	2022-04-21T04:42:26.133087-04:00 magnum-16947 magauthensrv: INFO:interfaces.control:Request received. Client [10.1.2.84], Method [handle_get_user_authentication], Args [], Kwargs [{'login_info': {'username': 'testuser', 'password': '********'}}] 2022-04-21T04:42:26.350121-04:00 magnum-16947 magauthensrv: INFO:interfaces.control:Authentication Failed.: testuser 2022-04-21T04:42:27.637534-04:00 magnum-16947 magauthensrv: INFO:interfaces.control:Request received. Client [10.1.2.84], Method [handle_get_user_authentication], Args [], Kwargs [{'login_info': {'username': 'testuser', 'password': '********'}}] 2022-04-21T04:42:27.638140-04:00 magnum-16947 magauthensrv: INFO:interfaces.control:Can't log in. Account is locked.: testuser
FIA_UIA_EXT.1	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	**Local Console Login:** **Good Password for SSH:** 2022-03-17T08:27:37.164978-04:00 magnum-16947 login[3888249]: pam_unix(login:session): session opened for user etdev by LOGIN(uid=0) **Bad Password for local console:**

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			 **Remote SSH Login:** **Good Password for SSH:**  **Bad Password for SSH:** 2022-03-17T08:34:05.396944-04:00 magnum-16947 sshd[3905696]: Invalid user testoffice from 10.1.2.84 port 34894 2022-03-17T08:34:05.397486-04:00 magnum-16947 sshd[3905696]: debug1: PAM: initializing for "testoffice" 2022-03-17T08:34:07.217402-04:00 magnum-16947 sshd[3905696]: debug1: userauth-request for user testoffice service ssh-connection method password [preauth] 2022-03-17T08:34:08.935912-04:00 magnum-16947 sshd[3905696]: Failed password for invalid user testoffice from 10.1.2.84 port 34894 ssh2 **Remote WEB Login:** 2022-10-06T05:45:02.917161-04:00 magnum-86432 magauthensrv: INFO:interfaces.control:Request received. Client [10.1.2.84], Method [handle_get_user_authentication], Args [], Kwargs [{'login_info': {'username': 'testuser', 'password': '********'}}]

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2022-10-06T05:45:03.137568-04:00 magnum-86432 magauthensrv: INFO:interfaces.control:Authentication Failed.: testuser
FIA_UAU_EXT.2	All use of identification and authentication mechanism	Origin of the attempt (e.g., IP address)	Refer to the FIA_UIA_EXT.1 above.
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	**Removal of trust anchor:** 2022-08-29T07:37:24.622581-04:00 magnum-86432 magsecurity: Starting to remove trusted CA certificate 2022-08-29T07:37:24.623321-04:00 magnum-86432 magsecurity: Resolving actual certificate file path 2022-08-29T07:37:24.624425-04:00 magnum-86432 magsecurity: Removing certificate file: /usr/local/share/ca-certificates/ Acumen_Root_ICA.crt 2022-08-29T07:37:24.625639-04:00 magnum-86432 magsecurity: Updating trusted certificate list 2022-08-29T07:37:25.828450-04:00 magnum-86432 magsecurity: Making stunnel instances reload their configuration 2022-08-29T07:37:25.907500-04:00 magnum-86432 magsecurity: Done removing trusted CA certificate **Unsuccessful attempt to validate certificate:** 2022-08-29T07:55:05.550335-04:00 magnum-86432 stunnel-rsyslog-out- 6514: LOG4[1024549]: CERT: Pre-verification error (err=20): unable to get local issuer certificate 2022-08-29T07:55:05.550351-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG4[1024549]: Rejected by CERT at depth=0: C=US, O=Acumen,

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			OU=CC, CN=EvertzKaliTestingCert 2022-08-29T07:55:05.550362-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG7[1024549]: TLS alert (write): fatal: unknown CA 2022-08-29T07:55:05.550372-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG3[1024549]: SSL_connect: ssl/statem/statem_clnt.c:1913: error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed **Trust Anchors can only be added or deleted**
FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update	None	2022-09-20T02:02:17.426567-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [upgrade server] 2022-09-20T02:03:41.698503-04:00 magnum-86432 configshell: INFO:configshell.system:Attempting to sanitize file: /home/configshell/good_image_and_signature/magnum-rootfs-21.10.5.efp **Failed Update Logs**: 2022-11-03T07:40:12.237723-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [upgrade server] 2022-11-03T07:41:55.000656-04:00 magnum-86432 efpinstall: ++ basename /home/configshell/modified_version_of_ legitimately_signed_os/ magnum-rootfs-21.10.5.efp 2022-11-03T07:41:55.001390-04:00 magnum-86432 efpinstall: + info 'EFP: magnum-rootfs-21.10.5.efp' 2022-11-03T07:41:55.001943-04:00 magnum-86432 efpinstall: +

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			echo 'EFP: magnum-rootfs-21.10.5.efp' 2022-11-03T07:41:55.002611-04:00 magnum-86432 efpinstall: + '[' -n 1 ']' 2022-11-03T07:41:55.003413-04:00 magnum-86432 efpinstall: + check_signature /etc/ssl/local/evertz-code-verification-public-key.pem /home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp /home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp.sig 2022-11-03T07:41:55.003961-04:00 magnum-86432 efpinstall: + PUBKEY=/etc/ssl/local/evertz-code-verification-public-key.pem 2022-11-03T07:41:55.004506-04:00 magnum-86432 efpinstall: + EFPFILE=/home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp 2022-11-03T07:41:55.005229-04:00 magnum-86432 efpinstall: + SIGFILE=/home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp.sig 2022-11-03T07:41:55.005761-04:00 magnum-86432 efpinstall: + info 'Checking signature...' 2022-11-03T07:41:55.006285-04:00 magnum-86432 efpinstall: + echo 'Checking signature...' 2022-11-03T07:41:55.006939-04:00 magnum-86432 efpinstall: + '[' '!' –e /home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp.sig ']' 2022-11-03T07:41:55.007585-04:00 magnum-86432 efpinstall: + '[' '!' -e /etc/ssl/local/evertz-code-verification-public-key.pem ']'

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2022-11-03T07:41:55.008184-04:00 magnum-86432 efpinstall: + '[' '!' -x /opt/magnum-security-suite/bin/verify_efp_signature ']' 2022-11-03T07:41:55.008803-04:00 magnum-86432 efpinstall: + /opt/magnum-security-suite/bin/verify_efp_signature /etc/ssl/local/ evertz-code-verification-public-key.pem /home/configshell/modified_version_of_legitimately_signed_os/ magnum-rootfs-21.10.5.efp.sig /home/configshell/modified_version_of_legitimately_signed_os /magnum-rootfs-21.10.5.efp 2022-11-03T07:41:55.009385-04:00 magnum-86432 efpinstall: <13> Nov 3 07:41:55 magsecurity: Verifying EFP /home/configshell/modified_version_of_legitimately_signed_os/ magnum-rootfs-21.10.5.efp and signature /home/configshell/modified_version_of_legitimately_signed_os/ magnum-rootfs-21.10.5.efp.sig using /etc/ssl/local/evertz-code-verification- public-key.pem 2022-11-03T07:42:00.612684-04:00 magnum-86432 efpinstall: + error 'Signature FAILED' 2022-11-03T07:42:00.613310-04:00 magnum-86432 efpinstall: + echo 'Signature FAILED' 2022-11-03T07:42:00.613922-04:00 magnum-86432 efpinstall: + exit 1
FMT_SMF.1	All management activities of TSF data.	None	**Ability to administer the TOE locally and remotely:** Refer to FIA_UIA_EXT.1 audit log evidence in this table. **Ability to configure the session inactivity time before session**

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			termination or locking: 2022-11-04T02:10:46.175065-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [set session timeout] 2022-11-04T02:10:48.986410-04:00 magnum-86432 configshell: INFO:configshell.shell:Running privileged command. Command [sudo -- /opt/magnum-security-suite/bin/set_interactive_session_timeout 1] 2022-11-04T02:10:49.029577-04:00 magnum-86432 magsecurity: Setting shell interactive session timeout to 1 minutes 2022-11-04T02:10:49.030807-04:00 magnum-86432 magsecurity: Done setting shell interactive_session timeout to 1 minutes 2022-11-04T02:10:49.031417-04:00 magnum-86432 magsecurity: Reloading magauthensrv 2022-11-04T02:10:49.039137-04:00 magnum-86432 magsecurity: Done reloading magauthensrv with new login expiry 1 **Ability to update the TOE, and to verify the updates using [digital signature] capability prior to installing those updates:** Refer to FPT_TUD_EXT.1 audit log evidence in this table. **Ability to configure the authentication failure parameters for FIA_AFL.1.:** *Lockout threashold configuration:* 2022-11-04T02:12:01.714434-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [set account lockout threshold]

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2022-11-04T02:12:06.721184-04:00 magnum-86432 configshell: INFO:configshell.shell:Running privileged command. Command [sudo -- /opt/magnum-security-suite/bin/set_account_lockout_threshold 3] 2022-11-04T02:12:06.726218-04:00 magnum-86432 magsecurity: Setting account lockout threshold to 3 2022-11-04T02:12:06.755580-04:00 magnum-86432 magsecurity: Setting security option policy account_lockout_threshold to 3 2022-11-04T02:12:06.757961-04:00 magnum-86432 magsecurity: Done setting security option policy account_lockout_threshold to 3 2022-11-04T02:12:06.763230-04:00 magnum-86432 magsecurity: Configuring /etc/security/faillock.conf to use account lockout threshold of 3 2022-11-04T02:12:06.764767-04:00 magnum-86432 magsecurity: Reloading magauthensrv 2022-11-04T02:12:06.772386-04:00 magnum-86432 magsecurity: Done setting account lockout threshold to 3 *User lockout duration configuration:* 2022-11-04T02:09:36.118494-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [set account lockout duration] 2022-11-04T02:09:41.849992-04:00 magnum-86432 configshell: INFO:configshell.shell:Running privileged command. Command [sudo -- /opt/magnum-security-suite/bin/set_account_lockout_duration 1] 2022-11-04T02:09:41.855247-04:00 magnum-86432 magsecurity: Setting account lockout duration to 1 minutes 2022-11-04T02:09:41.884970-04:00 magnum-86432 magsecurity: Setting security option policy account_lockout_duration to 1

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2022-11-04T02:09:41.887339-04:00 magnum-86432 magsecurity: Done setting security option policy account_lockout_duration to 1 2022-11-04T02:09:41.892851-04:00 magnum-86432 magsecurity: Configuring /etc/security/faillock.conf to use account lockout duration of 60 seconds 2022-11-04T02:09:41.894429-04:00 magnum-86432 magsecurity: Reloading magauthensrv 2022-11-04T02:09:41.901851-04:00 magnum-86432 magsecurity: Done setting account lockout duration to 1 **Ability to configure audit behavior (e.g., changes to storage locations for audit; changes to behavior when local audit storage space is full):** 2022-11-04T02:14:10.597201-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [save secure audit settings] 2022-11-04T02:14:10.599341-04:00 magnum-86432 configshell: INFO:configshell.shell:Running privileged command. Command [sudo -- /opt/magnum-security-suite/bin/save_secure_audit_server_config 10.1.2.84 2>/dev/null] 2022-11-04T02:15:28.423841-04:00 magnum-86432 magsecurity: Adding audit server IP address: 10.1.2.84 2022-11-04T02:15:28.424613-04:00 magnum-86432 magsecurity: Done saving audit server IP addresses to /var/lib/magnum-security-suite/secure-audit-logger/magsecauditlogger.conf

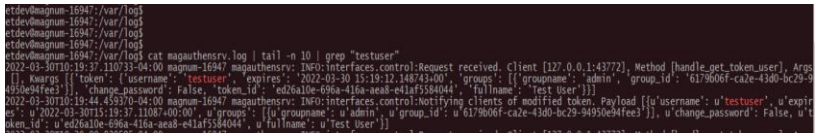
Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2022-11-04T02:15:28.425285-04:00 magnum-86432 magsecurity: Adding rsyslog UDP configuration file /etc/rsyslog.d/12-remote-tls-rsyslog-server.conf 2022-11-04T02:15:28.426467-04:00 magnum-86432 magsecurity: Done adding rsyslog UDP configuration file /etc/rsyslog.d/12-remote-tls-rsyslog-server.conf **Ability to manage the cryptographic keys.:** Refer to FMT_MTD.1/CryptoKeys Test #1 and FMT_MTD.1/CryptoKeys Test #2 **Ability to set the time which is used for timestamps:** Refer to FPT_STM_EXT.1 **Ability to import X.509v3 certificates to the TOE's trust store:** Refer to FIA_X509_EXT.1.1/Rev **Changing the login banner:** 2022-11-04T02:04:56.047512-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [edit login banner] **Resetting user passwords:** 2022-11-04T02:16:27.775889-04:00 magnum-86432 configshell: INFO:magsecurity:Performing privileged action. Client [10.1.2.84], Action [Changing password for user etdev]
FPT_STM_EXT.1	Discontinuous changes to time	For discontinuous	2022-10-21T10:55:32.951613-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action.

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
	- 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)	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).	Client [10.1.2.84], Action [change time] 2022-10-21T10:55:32.955292-04:00 magnum-86432 configshell: INFO:configshell.shell:Running privileged command. Command [sudo -- sed --follow-symlinks -i /'timestamp_timeout'/d /etc/ sudoers] 2022-10-21T10:55:32.978208-04:00 magnum-86432 configshell: INFO:configshell.shell:Running privileged command. Command [sudo – date 10211155.13] 2022-10-21T11:55:13.001054-04:00 magnum-86432 configshell: INFO:configshell.shell:Running privileged command. Command [sudo – sed --follow-symlinks -i /'timestamp_timeout'/d /etc/sudoers] 2022-10-21T11:55:19.777719-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [reboot and apply new time] 2022-10-21T11:55:19.779783-04:00 magnum-86432 configshell: INFO:configshell.shell:Running privileged command. Command [sudo -- shutdown -r now] 2022-10-21T11:58:18.574134-04:00 magnum-86432 configshell.maybe_resave_pacemaker_settings: INFO:configshell_cmd: Calling configshell function from command line. Version [8.0.6], Call [maybe_resave_pacemaker_settings()]
FPT_TUD_EXT.1	Initiation of update; result of the update	None	2022-09-20T02:02:17.426567-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84] , Action [upgrade server]

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
	attempt (success or failure)		2022-09-20T02:03:41.698503-04:00 magnum-86432 configshell: INFO:configshell.system:Attempting to sanitize file: /home/configshell/good_image_and_signature/magnum-rootfs-21.10.5.efp **Failed Update Logs**: 2022-11-03T07:40:12.237723-04:00 magnum-86432 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [upgrade server] 2022-11-03T07:41:55.000656-04:00 magnum-86432 efpinstall: ++ basename /home/configshell/modified_version_of_ legitimately_signed_os/ magnum-rootfs-21.10.5.efp 2022-11-03T07:41:55.001390-04:00 magnum-86432 efpinstall: + info 'EFP: magnum-rootfs-21.10.5.efp' 2022-11-03T07:41:55.001943-04:00 magnum-86432 efpinstall: + echo 'EFP: magnum-rootfs-21.10.5.efp' 2022-11-03T07:41:55.002611-04:00 magnum-86432 efpinstall: + '[' -n 1 ']' 2022-11-03T07:41:55.003413-04:00 magnum-86432 efpinstall: + check_signature /etc/ssl/local/evertz-code-verification-public-key.pem /home/configshell/modified_version_of_legitimately_signed_os/ magnum-rootfs-21.10.5.efp /home/configshell/modified_version_of_legitimately_signed_os/ magnum-rootfs-21.10.5.efp.sig 2022-11-03T07:41:55.003961-04:00 magnum-86432 efpinstall: + PUBKEY=/etc/ssl/local/evertz-code-verification-public-key.pem

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2022-11-03T07:41:55.004506-04:00 magnum-86432 efpinstall: + EFPFILE=/home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp 2022-11-03T07:41:55.005229-04:00 magnum-86432 efpinstall: + SIGFILE=/home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp.sig 2022-11-03T07:41:55.005761-04:00 magnum-86432 efpinstall: + info 'Checking signature...' 2022-11-03T07:41:55.006285-04:00 magnum-86432 efpinstall: + echo 'Checking signature...' 2022-11-03T07:41:55.006939-04:00 magnum-86432 efpinstall: + '[' '!' /home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp.sig ']' 2022-11-03T07:41:55.007585-04:00 magnum-86432 efpinstall: + '[' '!' -e /etc/ssl/local/evertz-code-verification-public-key.pem ']' 2022-11-03T07:41:55.008184-04:00 magnum-86432 efpinstall: + '[' '!' -x /opt/magnum-security-suite/bin/verify_efp_signature ']' 2022-11-03T07:41:55.008803-04:00 magnum-86432 efpinstall: + /opt/magnum-security-suite/bin/verify_efp_signature /etc/ssl/local/evertz-code-verification-public-key.pem /home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp.sig /home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp 2022-11-03T07:41:55.009385-04:00 magnum-86432 efpinstall: <13>Nov

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			3 07:41:55 magsecurity: Verifying EFP /home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp and signature /home/configshell/modified_version_of_legitimately_signed_os/magnum-rootfs-21.10.5.efp.sig using /etc/ssl/local/evertz-code-verification-public-key.pem 2022-11-03T07:42:00.612684-04:00 magnum-86432 efpinstall: + error 'Signature FAILED' 2022-11-03T07:42:00.613310-04:00 magnum-86432 efpinstall: + echo 'Signature FAILED' 2022-11-03T07:42:00.613922-04:00 magnum-86432 efpinstall: + exit 1
FTA_SSL.3	The termination of a remote session by the session locking mechanism	None	**SSH:** 2022-03-22T05:39:52.065166-04:00 magnum-16947 configshell: INFO:configshell.dialog.gui:Performing privileged action. Client [10.1.2.84], Action [set session timeout] 2022-03-22T05:40:31.466417-04:00 magnum-16947 configshell: INFO:configshell.shell:Running privileged command. Command [sudo -- /opt/magnum-security-suite/bin/set_interactive_session_timeout 1] **WebUI:** 

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTA_SSL.4	The termination of an interactive session	None	**SSH:** 2022-03-23T09:07:58.876668-04:00 magnum-16947 sshd[36725]: Disconnected from user etdev 10.1.2.84 port 35342 2022-03-23T09:07:58.876971-04:00 magnum-16947 sshd[36725]: pam_unix(sshd:session): session closed for user etdev **Local Console:**   **WebUI:**  
FTA_SSL_EXT.1 (if “terminate the session” is selected)	The termination of a local session by the session locking mechanism	None	**Session Timeout Log:** 2022-03-23T09:33:42.287308-04:00 magnum-16947 login[100547]: pam_unix(login:session): session closed for user etdev

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTP_ITC.1	• Initiation of the trusted channel • Termination of the trusted channel • Failure of the trusted channel functions	Identification of the initiator and target of failed trusted channels establishment attempt	**Initiation:** 2022-08-24T09:38:56.211305-04:00 magnum-86432 stunnel-magdrvsrv- ipx-exe-out-9672: LOG6[568469]: s_connect: connecting 10.1.2.84:9672 2022-08-24T09:38:56.211885-04:00 magnum-86432 stunnel-magdrvsrv- ipx-exe-out-9672: LOG5[568469]: s_connect: connected 10.1.2.84:9672 2022-08-24T09:38:56.211913-04:00 magnum-86432 stunnel-magdrvsrv- ipx-exe-out-9672: LOG5[568469]: Service [magdrvsrv-ipx-exe-out-9672] connected remote server from 10.1.2.253:52208 **Termination:** 2022-08-24T09:39:16.211739-04:00 magnum-86432 stunnel-magdrvsrv- ipx-exe-out-9672: LOG7[568469]: TLS alert (write): warning: close notify 2022-08-24T09:39:16.211752-04:00 magnum-86432 stunnel-magdrvsrv -ipx-exe-out-9672: LOG6[568469]: SSL_shutdown successfully sent close_notify alert **Failure:** **Logs when the connection initiated:** 2022-11-04T08:17:47.008188-04:00 magnum-86432 stunnel-rsyslog

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			-out-6514: LOG5[42109]: Service [rsyslog-out-6514] accepted connection from 10.1.2.253:56684 2022-11-04T08:17:47.008205-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: s_connect: connecting 10.1.2.84:6514 2022-11-04T08:17:47.008219-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG7[42109]: s_connect: s_poll_wait 10.1.2.84:6514: waiting 10 seconds 2022-11-04T08:17:48.032742-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG5[42109]: s_connect: connected 10.1.2.84:6514 2022-11-04T08:17:48.032787-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG5[42109]: Service [rsyslog-out-6514] connected remote server from 10.1.2.253:56692 2022-11-04T08:17:48.032882-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: Peer certificate required 2022-11-04T08:17:48.039156-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG7[42109]: CERT: Pre-verification succeeded 2022-11-04T08:17:48.039171-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: MAGNUM (CRL): Considering subject /C=US/O=Acumen/OU=CC/CN=AcumenICA 2022-11-04T08:17:48.039186-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: MAGNUM (CRL): Attempting to download URI http://10.1.2.84/Acumen_Root_ICA.crl to /tmp/crldp.mYXtgF/Acumen_Root_ICA.crl 2022-11-04T08:17:48.041662-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: MAGNUM (CRL): Download completed (URI: http://10.1.2.84/Acumen_Root_ICA.crl) 2022-11-04T08:17:48.162034-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: MAGNUM (CRL): Import of CRL from URI http://10.1.2.84/Acumen_Root_ICA.crl successful

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2022-11-04T08:17:48.162054-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: Checking CRL revocation status for cert /C=US/O=Acumen/OU=CC/CN=AcumenICA ... 2022-11-04T08:17:48.162140-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: MAGNUM (CRL): Successfull loaded 1 CRLs into stack.2022-11-04T08:17:48.162199-04:00 magnum-86432 stunnel- rsyslog- out-6514: LOG6[42109]: CERT: Host name "evertz.magnum.com" matched with "evertz.magnum.com" 2022-11-04T08:17:48.162216-04:00 magnum-86432 stunnel-rsyslog-out -6514: LOG5[42109]: Certificate accepted at depth=0: C=US, O=Acumen, OU=CC, CN=AcumenICA 2022-11-04T08:17:48.164849-04:00 magnum-86432 stunnel-rsyslog-out -6514: LOG6[42109]: Session id: 929A5C12A40BDA7011AB263E2F793B01F9281792807FBC08EBCA71A21DF94C45 2022-11-04T08:17:48.164925-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: TLS connected: new session negotiated 2022-11-04T08:17:48.164939-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42109]: TLSv1.2 ciphersuite: ECDHE-RSA-AES256-GCM- SHA384 (256-bit encryption) 2022-11-04T08:17:48.164953-04:00 magnum-86432 stunnel-rsyslog-out

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			-6514: LOG7[42109]: Compression: null, expansion: null **Logs When connection restored:** 2022-11-04T08:33:34.113603-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: s_connect: connecting 10.1.2.84:6514 2022-11-04T08:33:34.113615-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG7[42113]: s_connect: s_poll_wait 10.1.2.84:6514: waiting 10 seconds 2022-11-04T08:33:36.162468-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG5[42113]: s_connect: connected 10.1.2.84:6514 2022-11-04T08:33:36.162514-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG5[42113]: Service [rsyslog-out-6514] connected remote server from 10.1.2.253:34348 2022-11-04T08:33:36.168132-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG7[42113]: CERT: Pre-verification succeeded 2022-11-04T08:33:36.168143-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: MAGNUM (CRL): Considering subject /C=US/O=Acumen/OU=CC/CN=AcumenICA 2022-11-04T08:33:36.168155-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: MAGNUM (CRL): Attempting to download URI http://10.1.2.84/Acumen_Root_ICA.crl to /tmp/crldp.LbmH7F/Acumen_Root_ICA.crl 2022-11-04T08:33:36.170960-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: MAGNUM (CRL): Download completed (URI: http://10.1.2.84/Acumen_Root_ICA.crl) 2022-11-04T08:33:36.290326-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: MAGNUM (CRL): Import of CRL from URI http://10.1.2.84/Acumen_Root_ICA.crl successful

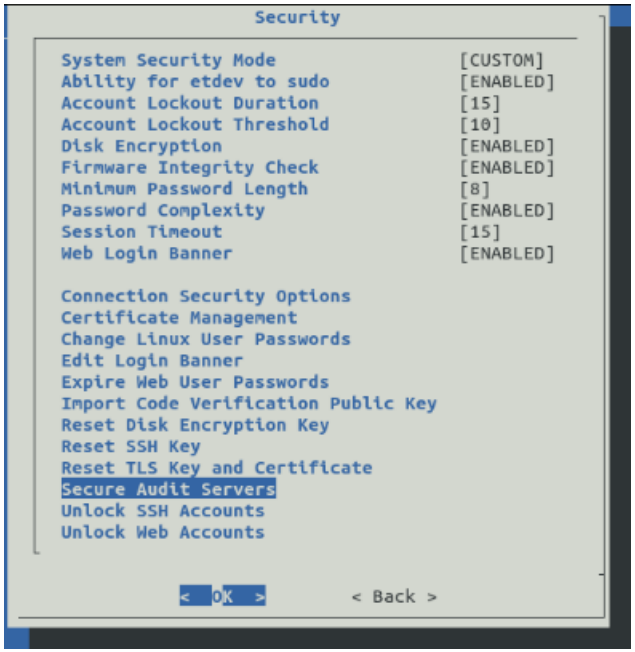
Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
			2022-11-04T08:33:36.290345-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: Checking CRL revocation status for cert /C=US/O=Acumen/OU=CC/CN=AcumenICA ... 2022-11-04T08:33:36.290383-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: MAGNUM (CRL): Successfull loaded 1 CRLs into stack. 2022-11-04T08:33:36.290453-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: CERT: Host name "evertz.magnum.com" matched with "evertz.magnum.com" 2022-11-04T08:33:36.290475-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG5[42113]: Certificate accepted at depth=0: C=US, O=Acumen, OU=CC, CN=AcumenICA 2022-11-04T08:33:36.293097-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: Session id: DB34776BB1B42C523CA0A496A471A2B360152204EF8447327F0B03E155C1159A 2022-11-04T08:33:36.293197-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: TLS connected: new session negotiated 2022-11-04T08:33:36.293217-04:00 magnum-86432 stunnel-rsyslog-out-6514: LOG6[42113]: TLSv1.2 ciphersuite: ECDHE-RSA-AES256-GCM-SHA384 (256-bit encryption)

Requirement	Auditable Events	Additional Audit Record Contents	Audit Record
FTP_TRP.1/Admin	• Initiation of the trusted path • Termination of the trusted path. • Failure of the trusted path functions.	None	**Initiation:** 2022-09-06T08:44:13.688407-04:00 magnum-86432 sshd[3506930]: pam_unix(sshd:session): session opened for user etdev by (uid=0) **Termination:** 2022-09-06T08:44:23.425597-04:00 magnum-86432 sshd[3507167]: Close session: user etdev from 10.1.2.84 port 42304 id 0 2022-09-06T08:44:23.425659-04:00 magnum-86432 sshd[3507167]: Disconnected from user etdev 10.1.2.84 port 42304 2022-09-06T08:44:23.426058-04:00 magnum-86432 sshd[3506930]: pam_unix(sshd:session): session closed for user etdev **Failure:** 2022-09-06T08:51:23.536802-04:00 magnum-86432 sshd[3532292]: debug1: PAM: password authentication failed for etdev: Authentication failure 2022-09-06T08:51:23.536836-04:00 magnum-86432 sshd[3532292]: Failed password for etdev from 10.1.2.84 port 42312 ssh2 2022-09-06T08:51:25.821346-04:00 magnum-86432 sshd[3532292]: Connection closed by authenticating user etdev 10.1.2.84 port 42312 [preauth]

14.2. Configuring Secure Audit Servers

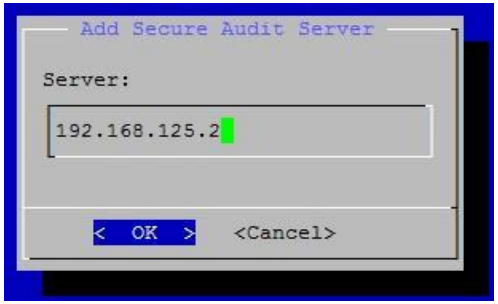
System log messages can be sent to a remote audit server. The remote audit server must listen on port **6514** for TLS connections, and its certificate chain must be trusted by MAGNUM in High Security Mode. All audit events are simultaneously sent to the remote server and the local store. If this or any outgoing client connection is unintentionally broken, MAGNUM will automatically reconnect within seconds.

1. Log in to the console as configshell and select Security
2. Select Secure Audit Servers



3. Select Add Server to add new entries

4. Enter a valid IP address

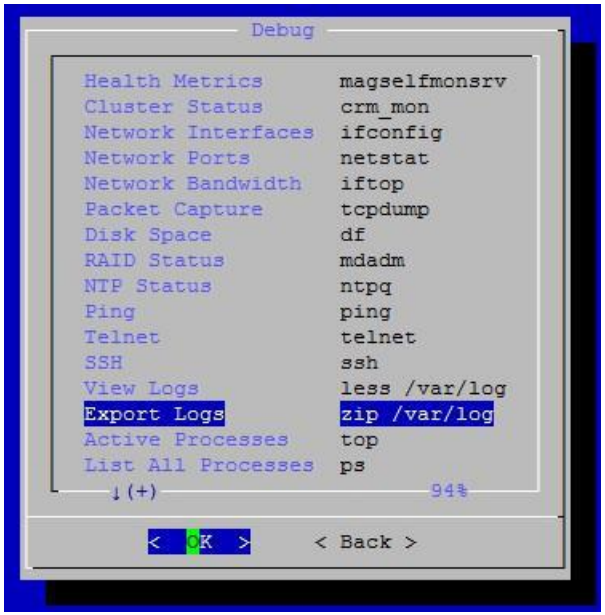


5. Add additional servers as needed
6. Remove a server by selecting it and erasing the IP address value
7. Select Save and Apply
8. When prompted, enter configshell's password
9. The change will take effect immediately

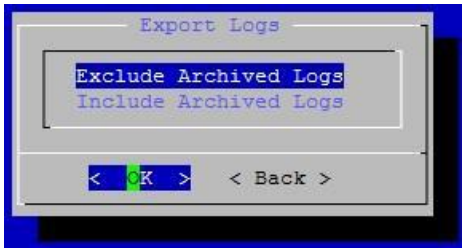
14.3. Export Logs

Export local audit logs for off-site review.

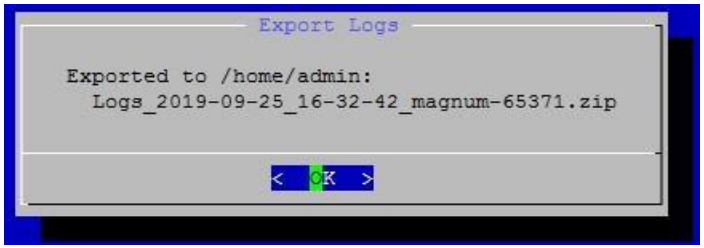
1. Log in to the console as configshell and select Debug
2. Select Export Logs



3. Decide whether to exclude or include archived logs



4. When prompted, enter configshell's password
5. Select the destination, either /home/admin via SFTP or USB Device
6. Wait until the export completes

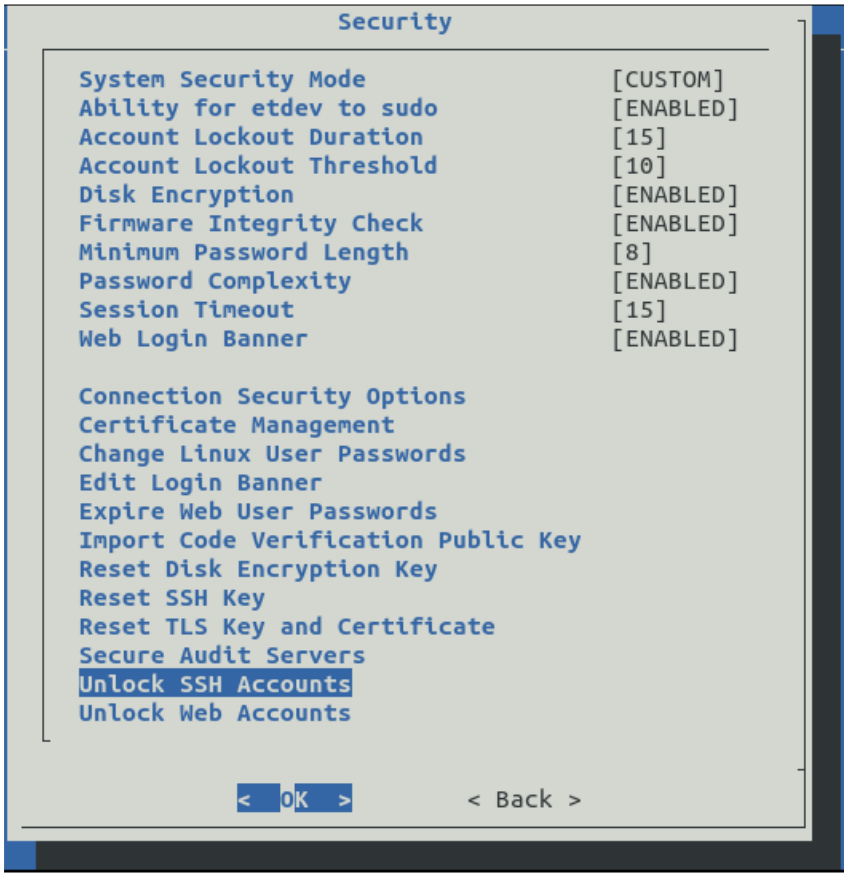


15. UNLOCKING LOCKED ACCOUNTS

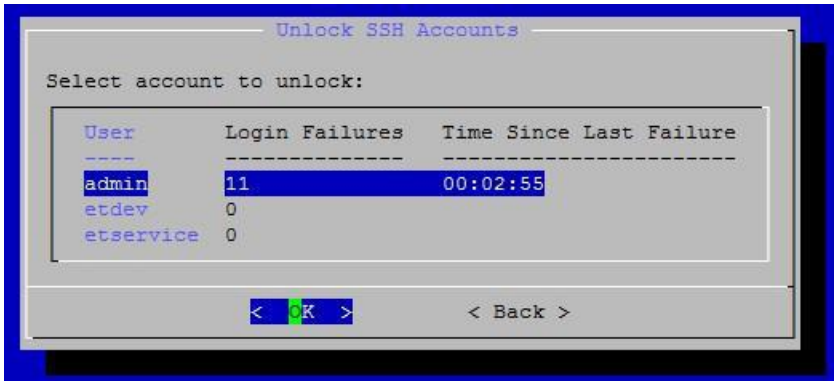
15.1. Unlock SSH Accounts

Unlock SSH user accounts that have been locked due to too many failed login attempts.

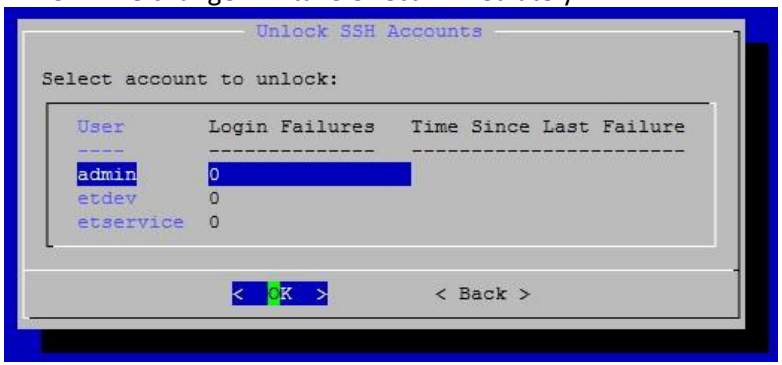
1. Log in to the console as configshell and select Security
2. Select Unlock SSH Accounts



3. Select the user account to unlock



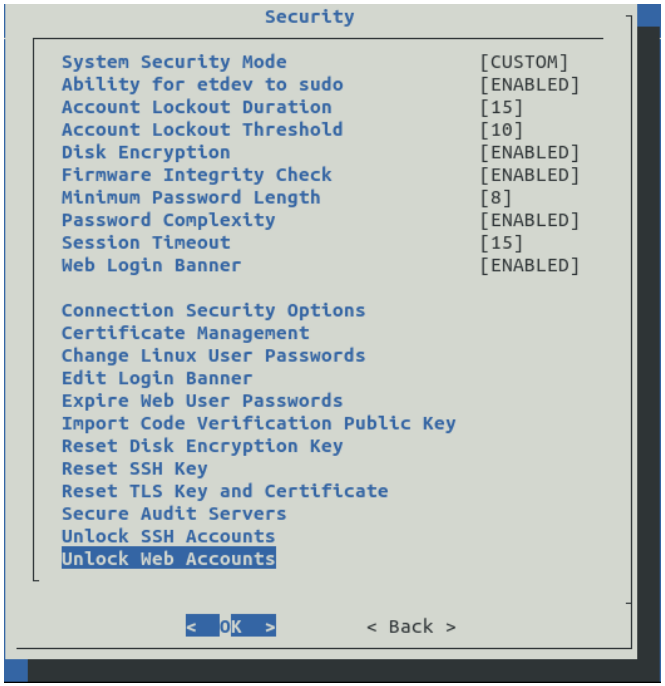
4. When prompted, enter configshell's password
5. The change will take effect immediately



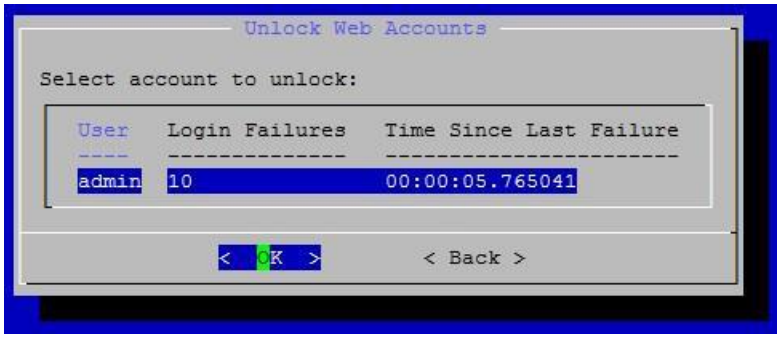
15.2. Unlock Web Accounts

Unlock web user accounts that have been locked due to too many failed login attempts.

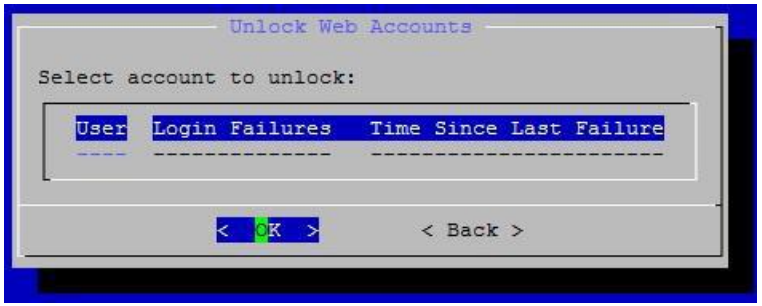
1. Log in to the console as configshell and select Security
2. Select Unlock Web Accounts



3. Select the web user account to unlock



4. When prompted, enter configshell's password
5. The change will take effect immediately

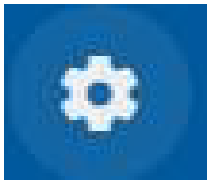


16. USER MANAGEMENT

16.1. Create and Remove Web Users

The **admin** web user can create and remove non-admin web users. These users have limited access, and cannot change any sensitive configuration (except for their own passwords).

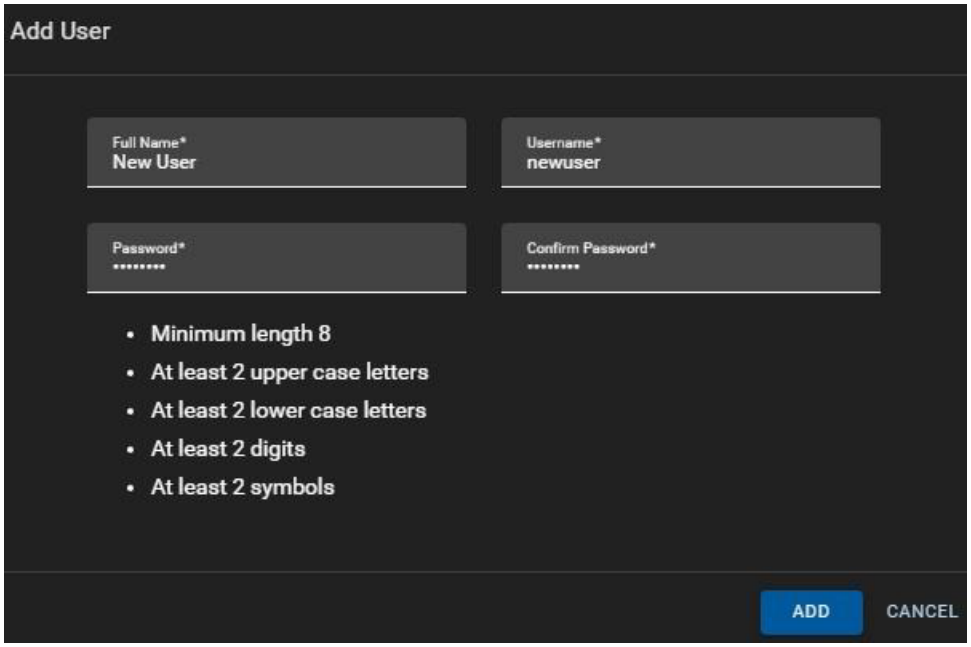
1. Log in to the web interface as admin
2. Select the configuration icon on the top right of the web page



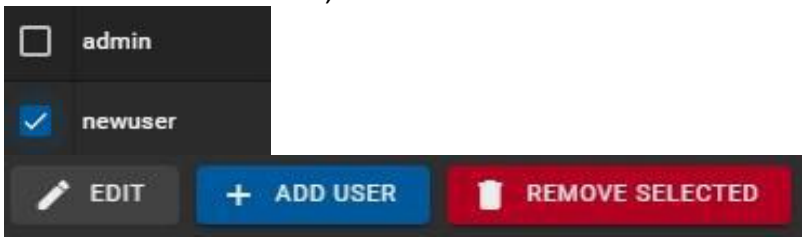
3. Select Users from the left menu

4. Select Add User from the bottom menu

5. Complete all fields and select Add



6. To remove a user, check the box beside the user name, and select Remove Selected



16.2. Change Web User Passwords

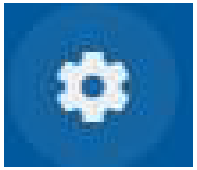
Web users can change their own passwords. The **admin** web user can also change every other web user's password. Every web user's password is automatically expired when entering High Security Mode (including admin), or when they are explicitly expired from the console menu.
In High Security Mode, all web and console passwords must meet increased complexity requirements:

- Minimum length 8 characters
- Must use two of each
    - Upper case letters
    - Lower case letters
    - Numbers
    - Symbols
- No reusing previous password

The allowed character list is:

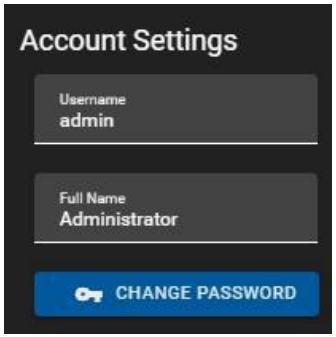
- Upper case letters
- Lower case letters
- Numerals
- Special characters
- [“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”]
- Other special characters:
- [“ “, “””, “‘”, “+”, ”,”, ”-”, ”.”, ”/”, ”:”, ”;”, ”<”, ”=”, ”>”, ”?”, ”[“, ”\”, ”]”, ”_”, ”`”, ”{“, ”|”, ”}”, ”~”]

1. Log in to the web interface as any user
2. Select the **configuration icon** on the top right of the web page

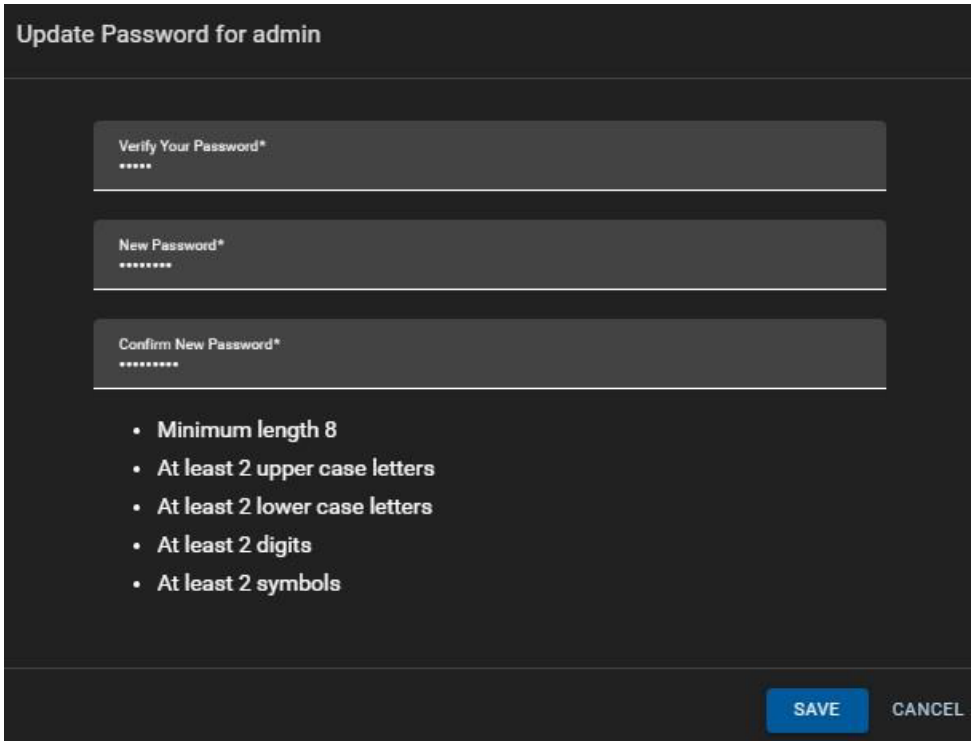


3. Select **Account** from the left menu to modify the currently logged in account

4. Select Change Password



5. Complete all fields and select **Save**



17. DATA PURGE

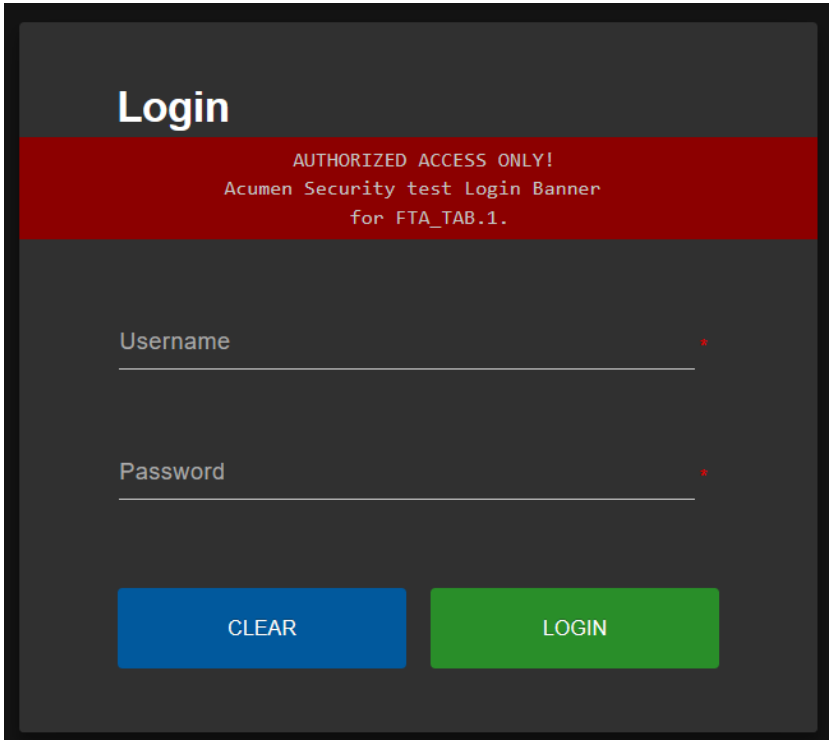
If the device needs to be to fully purged:

1. Power down the device
2. Remove both SSDs located at the back of the device
3. Place the SSDs into a hard drive shredder
4. Contact either sales or service at Evertz to get replacement SSDs

Software methods of securely erasing files are not guaranteed to be totally effective. There is no method to manually clear or purge old audit logs from the device.

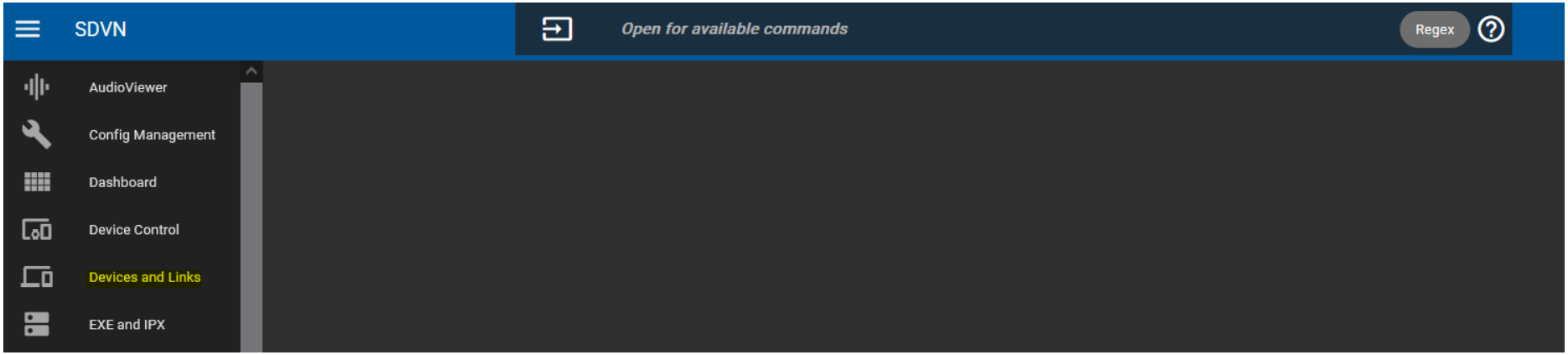
18. CONFIGURATION OF IPX CHANNEL

1. Log in to the Magnum through WebUI

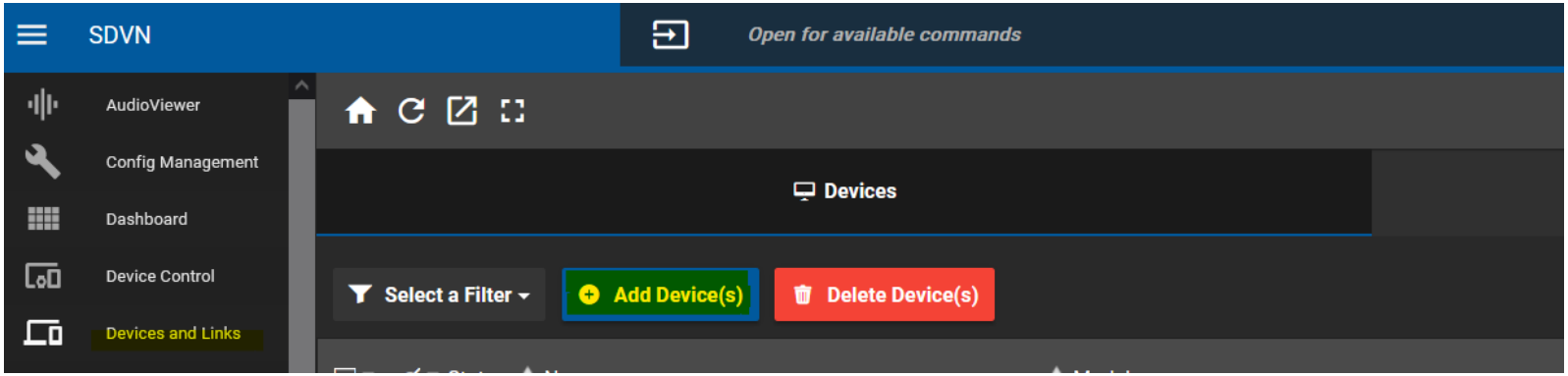


2. Select the System type as SDVN

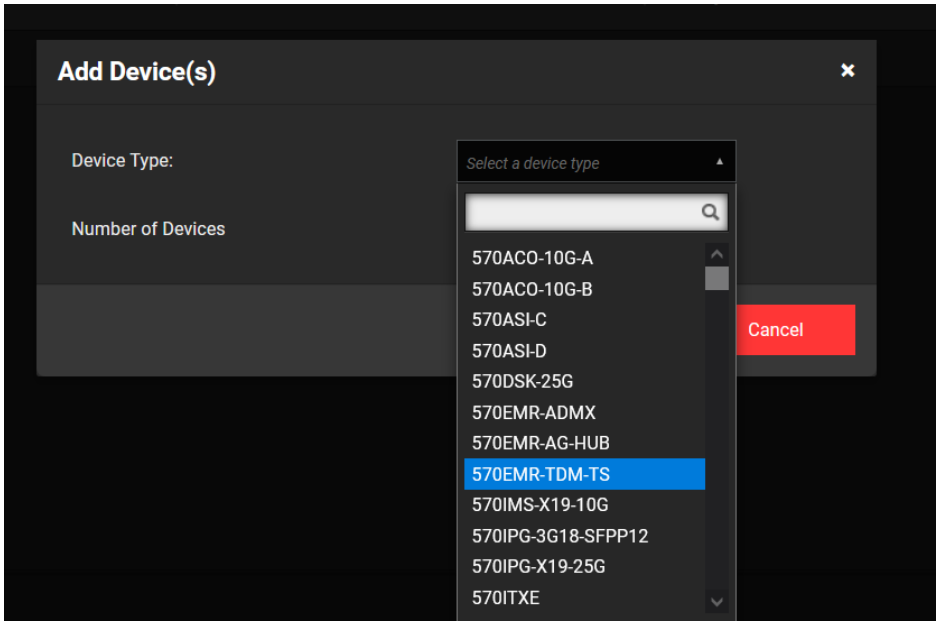
3. Click on Devices and Links:



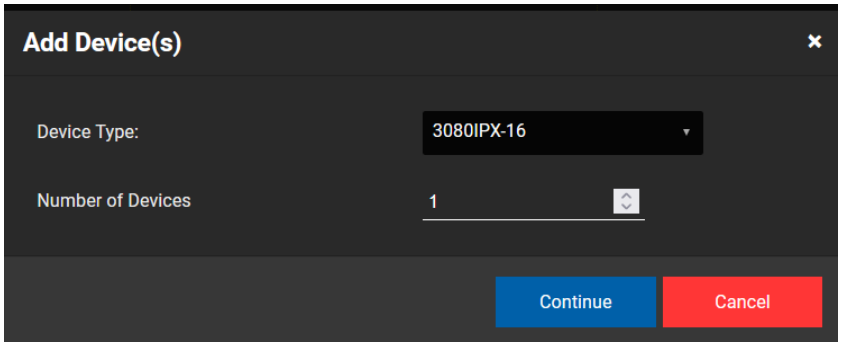
4. Click on Add Device(s)



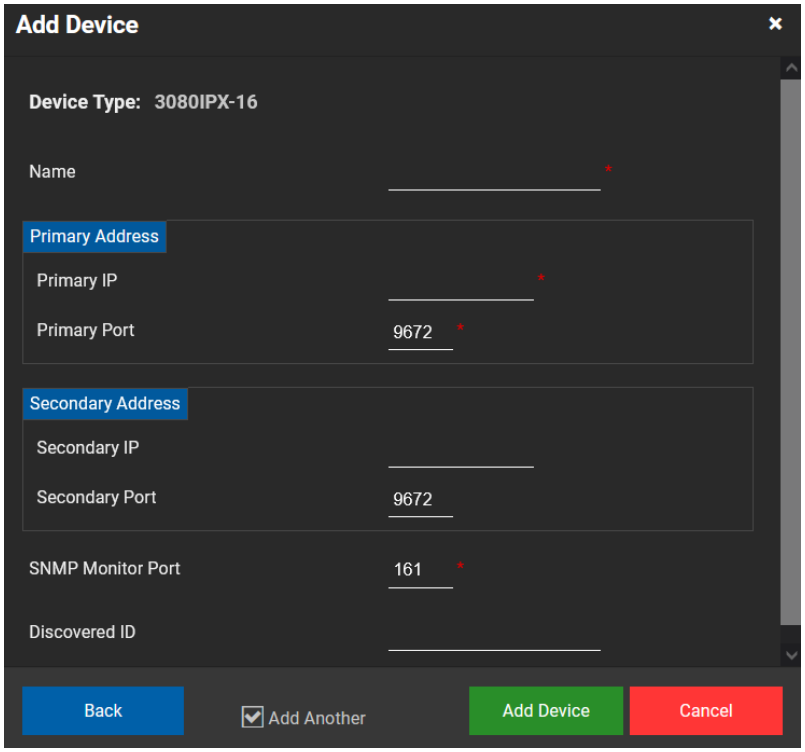
5. Select the required Device Type:



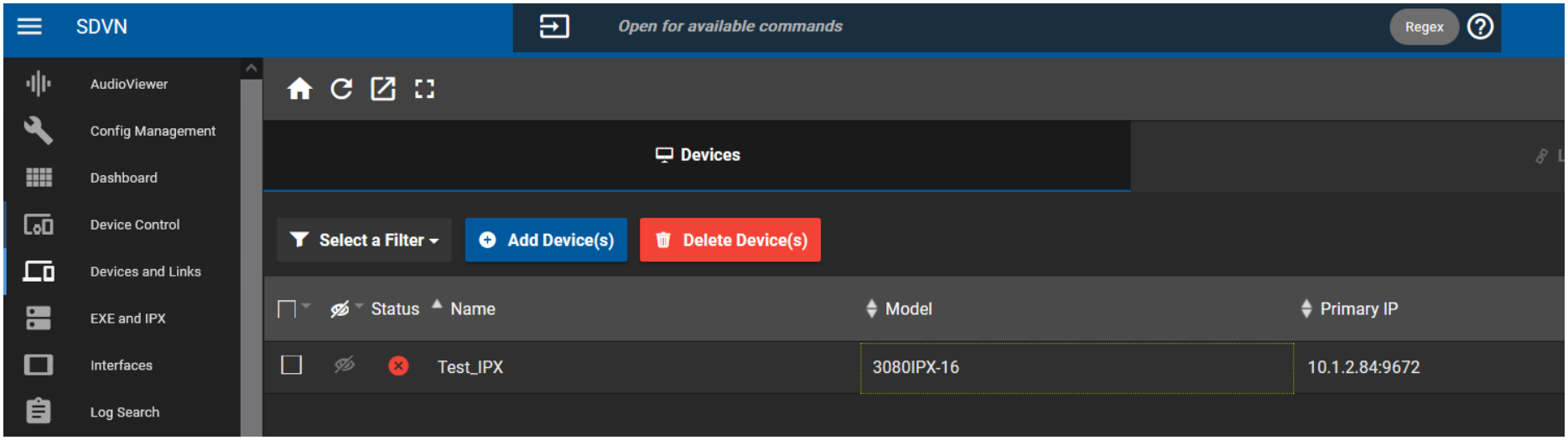
6. Select the Number of Devices:



7. Enter device details and click on Add Device



8. The device is added:


SDVN
Open for available commands
Regex
AudioViewer
Config Management
Dashboard
Device Control
Devices and Links
EXE and IPX
Interfaces
Log Search
Devices
Select a Filter
Add Device(s)
Delete Device(s)
Status
Name
Model
Primary IP
Test_IPX
3080IPX-16
10.1.2.84:9672