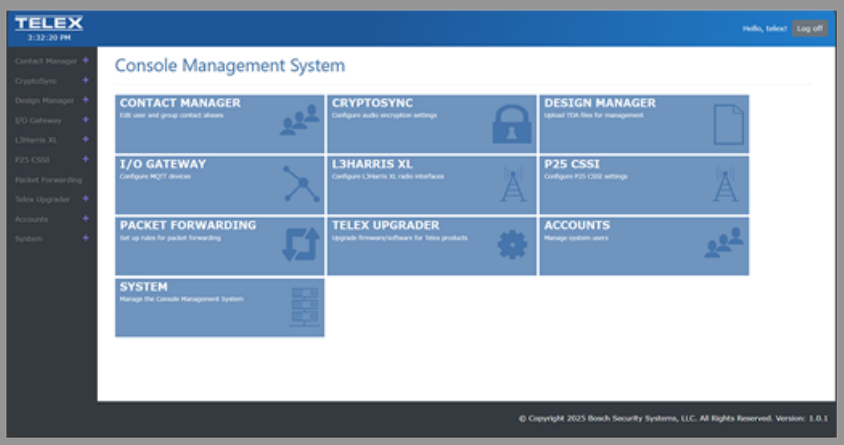
Console Management System

TCMS - Console Management System



en Technical Manual

Table of contents

1 Notices

1.1 Proprietary notice

The product information and design disclosed herein were originated by and are the property of Bosch Security Systems, LLC. Bosch reserves all patent, proprietary design, manufacturing, reproduction, use and sales rights thereto, and to any article disclosed therein, except to the extent rights are expressly granted to others.

1.2 Copyright notice

1.3 Warranty notice (limited)

For warranty and service information, see http://www.telex.com/warranty.

1.4 Factory service center

Factory Service Center
Bosch Security Systems, LLC
Radio Dispatch Products
140 Caliber Ridge Drive
Greer, SC 29651

1.5 Contact information

Sales
E-mail: TelexDispatch@ keenfinity-group.com
Phone: (800) 289-0096

Customer service repair
E-mail: repairservice.nam@keenfinity-group.com
Phone: (800) 553-5992

Technical support
E-mail: TelexDispatchtechsupport@ keenfinity-group.com
Knowledge database: http://knowledge.keenfinity-group.com/
Web: www.telex.com

1.6 Claims

No liability will be accepted for damages directly or indirectly arising from the use of our materials or from any other causes. Our liability shall be expressly limited to replacement or repair of defective materials.

1.7 Warning

Notice!
This is a class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

1.8 PC & Network Security consideration

No system can be 100% protected against security threats. However, there are measures both manufacturers and users can do to help reduce the likelihood of a malicious attack resulting in either the loss of data or system takeover. We evaluate and improve our products continuously to protect against such attacks. This is only one safeguard used to reduce the likelihood of such an event. There are many more considerations needed to implement measures to strengthen your network security. We strongly recommend the following considerations:

- Deploy Dispatch products and software on isolated networks that do not connect to other networks, when possible.
- Apply the latest Windows updates and install up-to-date IT security software.
- User rights should be properly administered using group policies to prevent unauthorized use of USB connected devices.
- If the Dispatch network must connect to other networks, install and properly maintain firewalls and intrusion detection systems.
- If Dispatch devices or computers use the Internet to connect, a VPN or tunnel connection should be utilized. Examples of such products are those made by DCB (Data Communications for Business), Cisco, and others.

Notice!
Telex recommends utilizing the services of IT professionals knowledgeable about network design and the Linux operating system when configuring a Console Management System PC.

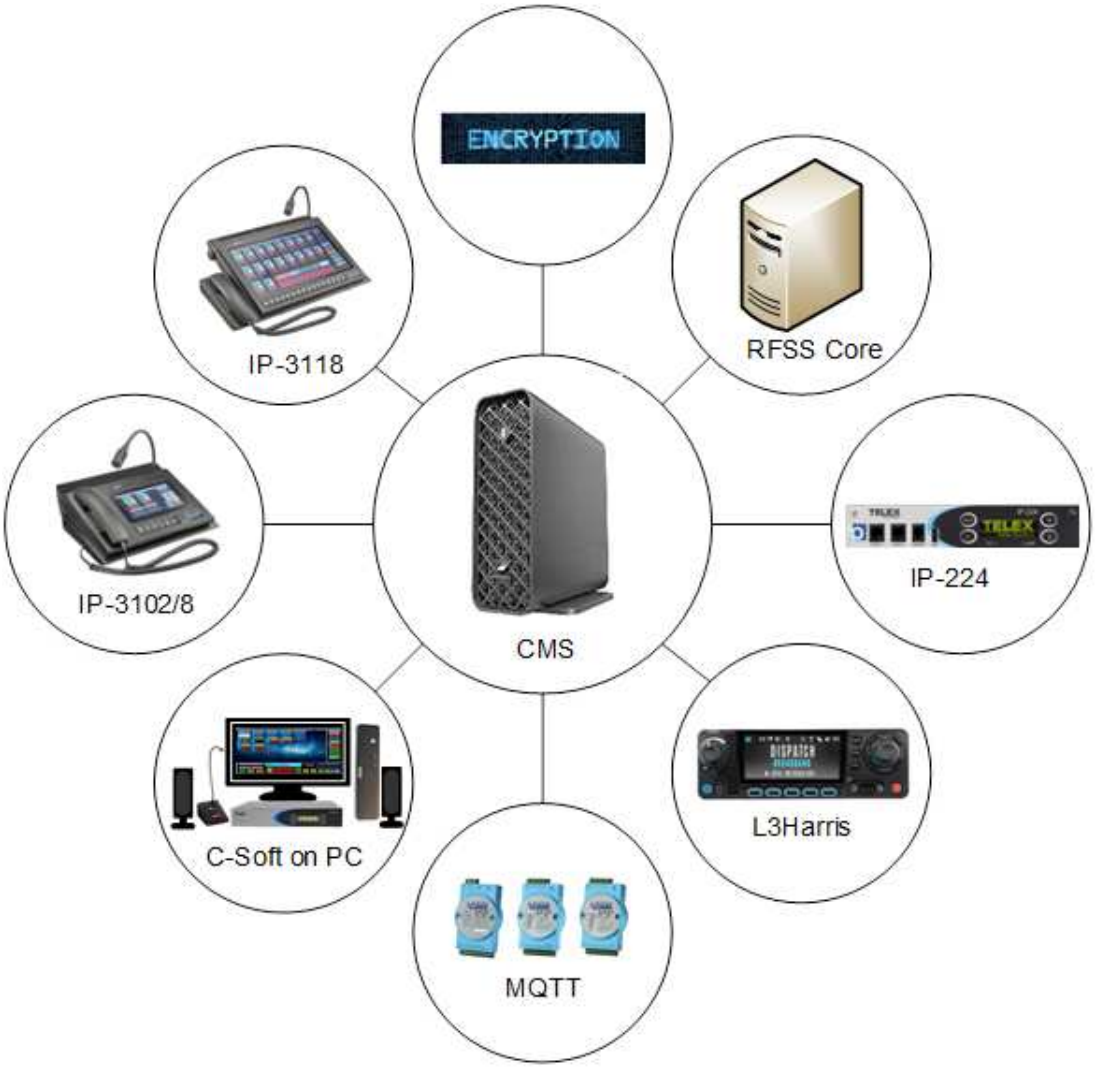
2 Introduction

Console Management System uses a 10th generation Intel i7 processor and CentOS 8 Stream Linux operating system to deliver high performance and stability for Telex Radio Dispatch systems.
The Console Management System is hosted on a centralized web server and sold as a Device and a; separate functional license is required. We will offer two functional licenses, I/O only will only support MQTT functionally while Core will support all standard functionally and 5 console connections included. Additional console connections can be ordered at any time when the system grows above 5.

Features

- Contains an 8 core CPU and an NVME M.2 SSD to optimize performance.
- CMS offers system management capabilities never offered before in a Telex Dispatch system. Supplied on a high availability Linux based server creating a centralized system management point supporting the following software features.
- Radio ID/Alias and SIP Phone book contact management with push functionally.
- C-Soft and IP-3000 series design management of TDA - Telex Design Archive files
- Management of user accounts to control TDA access.
- Encryption of IP packets between IP-224, IP-3100's, IP-3000's and C-Soft using AES-256 for voice protection.
- Packet Forwarding to convert Multicast to Unicast traffic (Echo Packets)
- Support MQTT I/O devices to expand or replace NEO-10.
- Support redundancy with synchronization and Auto-Failover when second CMS is installed in the system.
- Supports direct IP connection to L3Harris XL mobiles, sold as optional licensed feature and up to 20 radio connections can be supported. L3Harris XL-Link and XL-WAN Mobile licenses are required in each radio.
- Operate as the CSSI Gateway for connection to Motorola, Tait or L3Harris P25 cores, sold as optional licensed feature. Up to 100 Talk-Group registrations supported with 60 concurrent talk paths.
- Update C-Soft application on dispatch positions remotely. No longer go to each position to install updates. Requires positions to be updated to C-Soft version 8.2 or higher.
- Update firmware on IP-3000's, IP-224 and ADHB-4 devices remotely. Functions like Telex System Manager from a single system management platform.

3 System overview



4 Quick Installation

Required Equipment

– Console Management System Workstation

Workstation Setup and Configuration

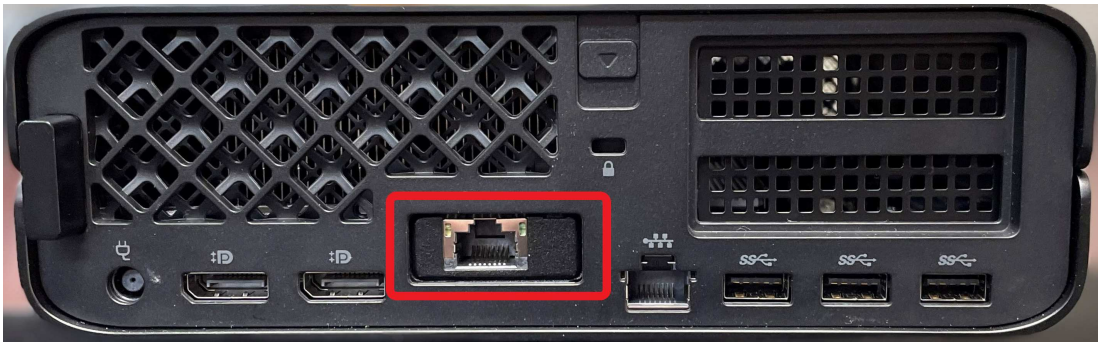
Box Contents

– 1 x Console Management System Workstation
– 1 x AC Power Adapter

Hardware Setup

1. Unbox the **CMS (Console Management System) Unit**.
2. Connect the **CMS unit to the power adapter**.
3. Plug **power adapter** into a wall socket.
4. Connect the **CMS unit directly to a laptop/PC** or **network switch with no gateway** with an Ethernet cable.
   The network adapter on the laptop/PC should be set to DHCP.
5. Disconnect or disable other **network connections**, on the connected laptop or PC if connected. It is recommended to disconnect or disable for proper IP routing.

Notice!
The configuration process only enables one specific network port. Use the network port, as shown in the picture.



CMS Configuration

Connect the device directly to a laptop or PC that has DHCP enabled or a network switch with no gateway. A laptop with DHCP enabled is still required if using a switch. When using DHCP on a flat network/direct connection, it can take up to two minutes for the network adapter to set the IP to a 169.254.X X address for a laptop or PC.

Notice!
Do not start the configuration until the IP address is assigned to the connected PC.

Requirements when using a failover system (two CMS servers):

– You must use a network switch
– Both servers must be on the same network as the configuration laptop or PC. The device will not be configured properly if the configuration is running separately with no inter-server communication.

To **configure the CMS device**, do the following:

1. Access the CMS server by **opening a web browser** (Internet Explorer not supported) and navigating to the device's default IP address, in the form of http://169.254.x.x. A label, found on the bottom of the unit, shows the default IP address of the CMS device.
   - If setting up failover, the second server IP will be in the form of http://169.254.x.x and have a label found on the bottom of the unit.
   - When setting up failover, submit the configuration for the primary server first, and then immediately repeat the steps to submit the configuration for the secondary server. The first server waits until the secondary server configuration has been submitted. It is recommended to submit one after another with minimal delays in between.
2. Click **Let's Go and accept the EULA**.
   The CMS configuration fields appear, which include the following:
   - Linux Root Password
   - Linux User(telex) Password
   - Network Adapter selection
   - IP Address
   - Subnet
   - Gateway
   - DNS Server
   - IPv6 configuration (not required)
   - NTP
   - Date (if not using NTP)
   - Time (if not using NTP)
   - Time zone
3. Select the **Using Failover** check box, if applicable.

Notice!
After configuration, the cluster will operate correctly without any additional setup. However, it is highly recommended to add fencing to the cluster.

Notice!
The Linux root and user passwords are important passwords and should be written down and placed into a safe location. They are not resettable or recoverable. If lost, the server would need a full factory restoration and would result in the loss of existing data.

4. Enter the **Linux Root password** you want to use.

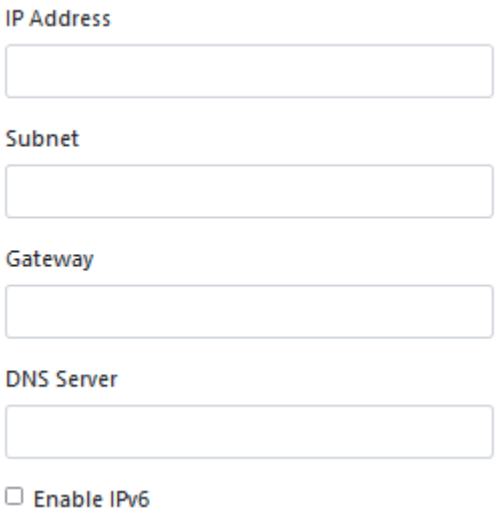
5. Enter the **Linux User password** you want to use.
   The default Linux username is **telex**.

Notice!
The OS passwords are separate from the website credentials.

6. Select the **Ethernet adapter** to configure.

Notice!
When selecting the network adapter, the status of each adapter appears. Select the one that is "Up". This is the network adapter that is used for configuration.

7. Set the **IP address, Subnet address, Gateway address, and the DNS address**.
   You can also set the IPv6 configuration, but it is not required.

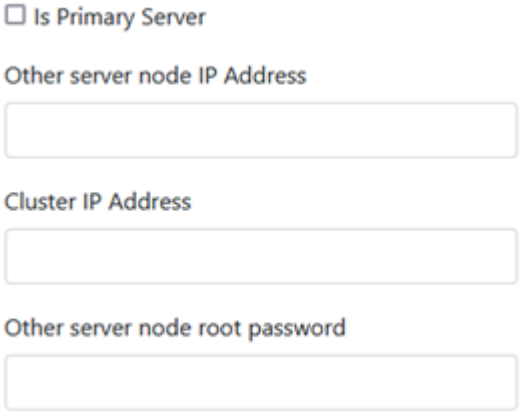


Notice!
You can also set the IPv6 configuration, but it is not required.

8. If using failover, the following fields appear.
   - Select the **Is Primary Server** check box to set the primary server.

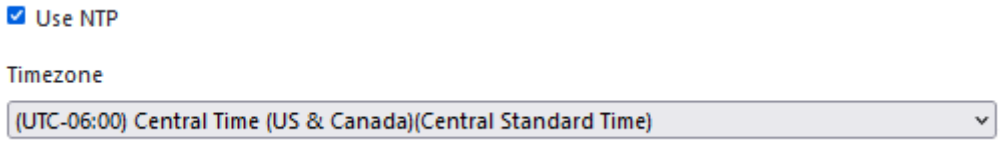
Notice!
Set only one server as the primary server. If both are set, the cluster configuration will fail.

   - **Other server node IP Address:** Enter the IP address the other server node uses.
   - **Cluster IP Address:** Enter the IP address to use for the cluster (this must match on both server configurations).
   - **Other server node root password:** Enter the root password that will be set on the other node.



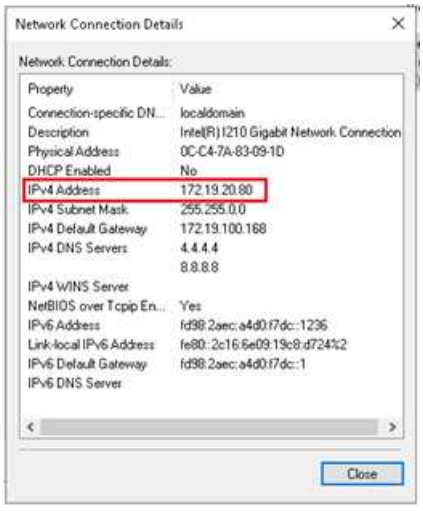
Notice!
By default, NTP is enabled on the device and the date time field are not shown. If you choose to set your own date and time, clear the NTP check box and set those fields.

9. Set the **time zone** for the server.



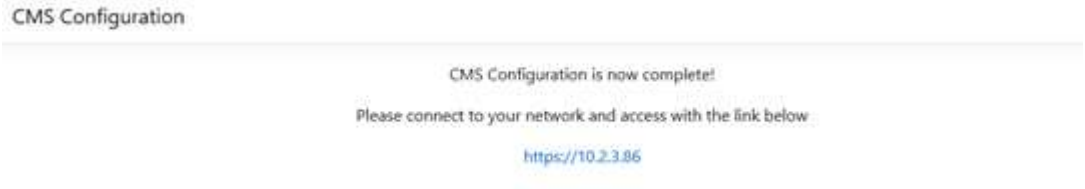
10. Click **Configure**.
    If there are errors in the form, they display in the form at this time. If there are no errors, a confirmation dialog appears. (Additional fields appear if using IPv6, failover or setting time manually).

11. Click **Submit**.
    Configuration of CMS starts. Once it finishes a message appears.
12. When using failover, the page redirects, an error in the web browser that a connection could not be made appears. Disconnect the Ethernet cable of the laptop/PC and reconnect. Make sure the Laptop/PC gets a new IP address



13. Refresh the page for both primary and secondary web pages.
14. Configuration continues.
    A progress bar shows on each server. When both have successfully finished you may continue.
15. Once finished, connect your **laptop/PC back to the network**.

16. Connect the **CMS unit(s)** to the network.
17. Click the **link** to access the CMS website.



Notice!
This process can take up to five minutes. If it takes longer, disconnect the Ethernet port and plug into the network.

18. Once the webpage launches, you will need to **install CMS license(s)** in order to operate the system.

5 CMS License Installation

Overview

These instructions are intended for a customer purchasing a Telex Console Management System or has purchased an upgrade license to enable a new feature for their device.

Equipment

Prior to receiving these instructions, you should receive one or more emails containing Entitlement Certificates. The Entitlement Certificates contain one or more Activation IDs. Activation IDs look like software serial numbers in the form of xxxxx-xxxxx-xxxxx-xxxxxx-xxxxx-xxxxx-xxxxxx.

Requirements

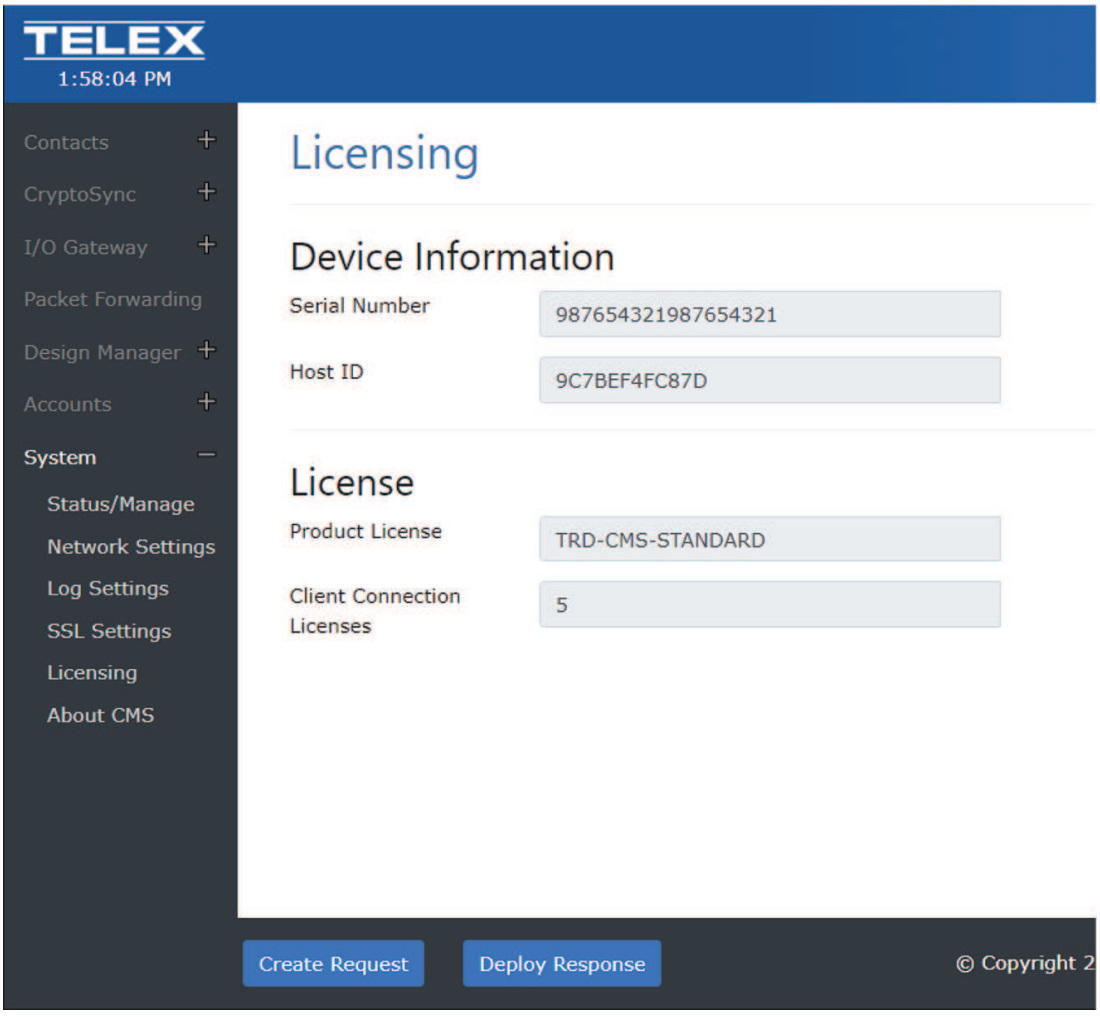
- Console Management System after initial setup stage
- One or more Activation IDs
- Activation to Bosch System Activation Website (https://licensing.boshcsecurity.com)
- Username and password for System Activation Website

Licensing Instructions

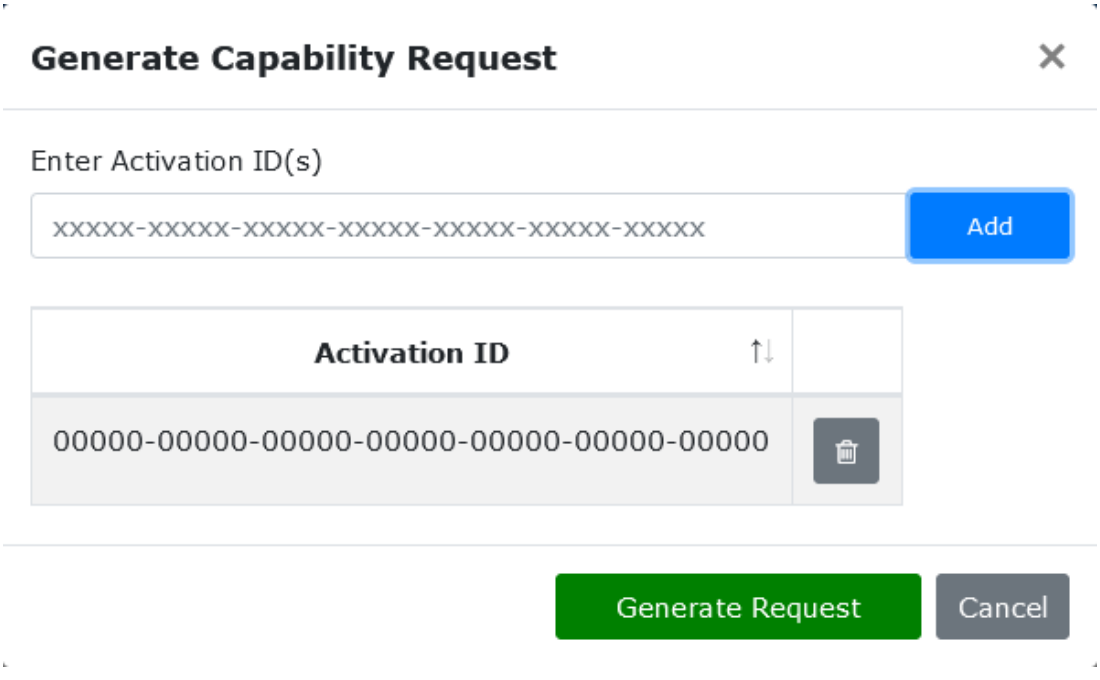
To **license the Console Management System**, do the following:

1. Open a **web browser** and navigate to the **CMS website**.
2. Enter a **valid username and password** to log onto the CMS webpage.
3. Navigate to **System | Licensing**.
   The Licensing page opens.

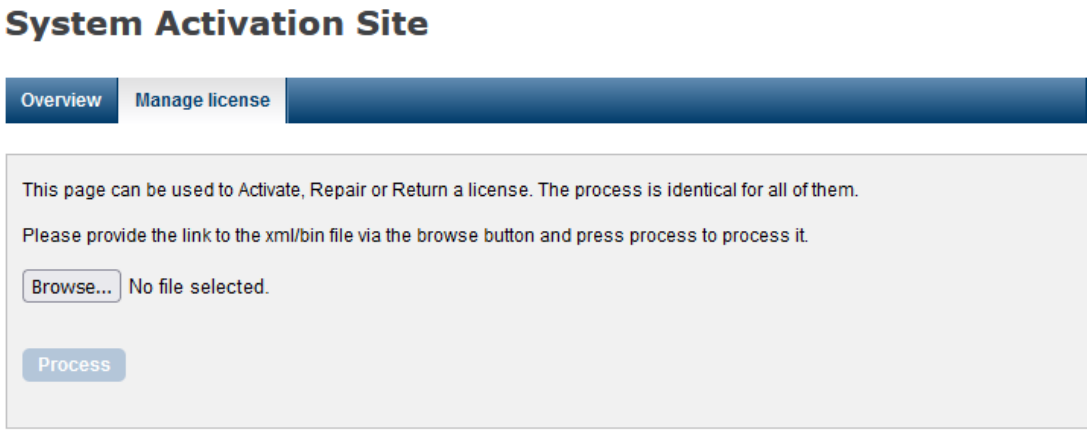
NOTE: If installing fail-over (two CMS), only have one unit attached at a time while licensing. Once you complete licensing on one unit, disconnect the unit and proceed to license the second unit.



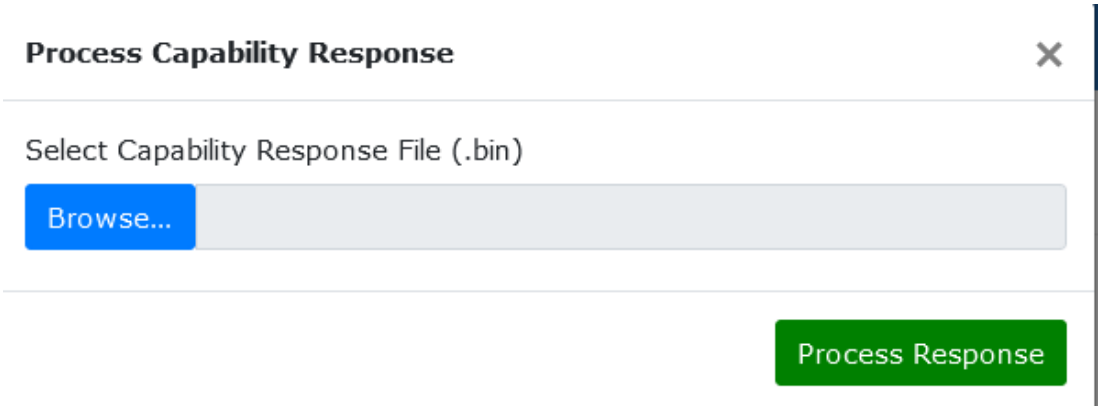
1. Click the **Create Request button** at the bottom of the page.
   The Generate Capability Request screen opens.



2. For each Activation ID, enter the **Activation ID** and then press **Add** to add it to the list of Activation IDs.
3. When finished, press the **Generate Request button**.
   You will be prompted to download the CapabilityRequest_XXXXXXXXXXX.bin, where the Xs match the CMS' Host ID. Save the file to a local, easily accessible location. Leave the CMS Licensing page open for later use.
4. Open the **Bosch System Activation website** (https://licensing.boschsecurity.com)
5. Login using your **username and password**.
6. Navigate to the **Manage license page**.



7. Press the **Browse button**.
8. Select the **ResponseRequest.XXXXXXXXXXX.bin**.
9. Click the **Process button.**
   You will prompted to download the CapabilityRequest_XXXXXXXXXXX.bin.
10. Click the **Deploy Response button** at the bottom of the page.
    The Process Capability Response screen opens.



11. Click the **Browse button**.
12. Navigate to and select the **ResponseRequest_XXXXXXXXXXX.bin file**.
13. Click the **Process Response button**.
    The Status text box displays feedback information from the license deployment procedure.
14. Click the **Close button**.
    The newly deployed license displays on the CMS Licensing page. The new license has been applied and the new features are now available.

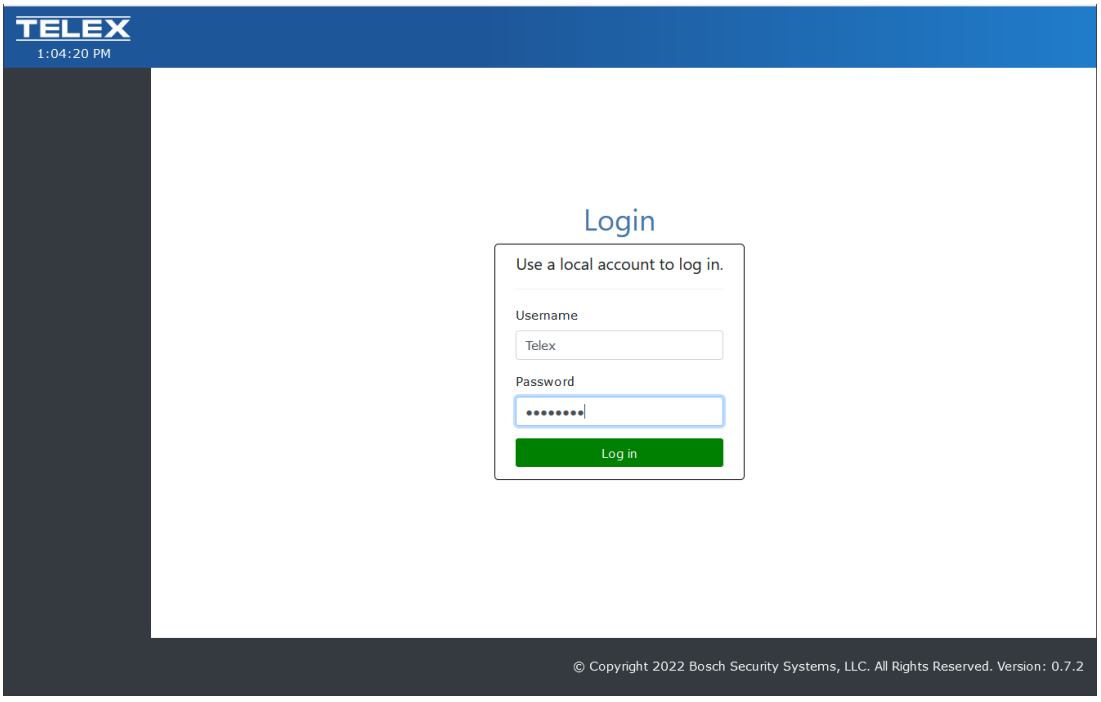
6 Logging In

6.1 Initial Login

Logging in to CMS for the first time, use the following login credentials:
Default username: telex
Default password: telex123
Once you have logged in, you must change the password immediately.
Passwords must have at least six characters

To **log into the server**, do the following:

1. In the Browser address field, enter the **IP Address of the server**.
2. Press the **Enter key**.
   The Login screen appears.

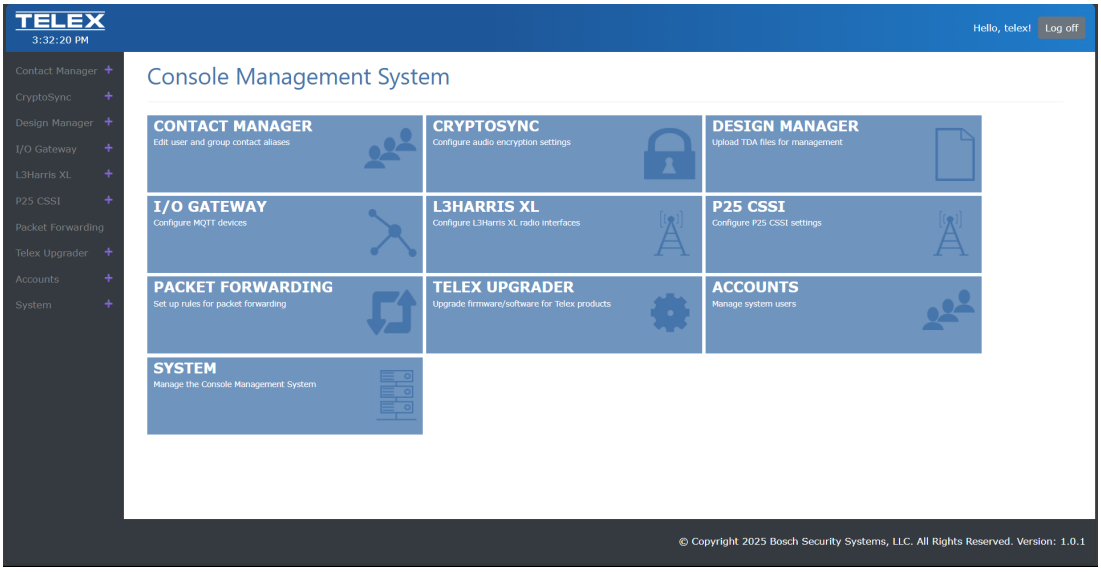


3. Enter the **default username**.
4. Enter the **default password**.
5. Click the **Login button**.
   The Change Password screen appears.

6. Enter your **new password**.
7. Re-enter your **new password to confirm**.
8. Click the **Set password button**.
   The Homepage opens.

6.2 Home page

After changing your password, the homepage opens. From this page, you can access each of the modules, as well as the system management page.



7 Account Management

Use the **Accounts Page** to access, manage, and maintain user profiles and roles in the system. If you are an administrator, you also can access user, role, and permission management pages. Otherwise, you can only have access to your own profile.

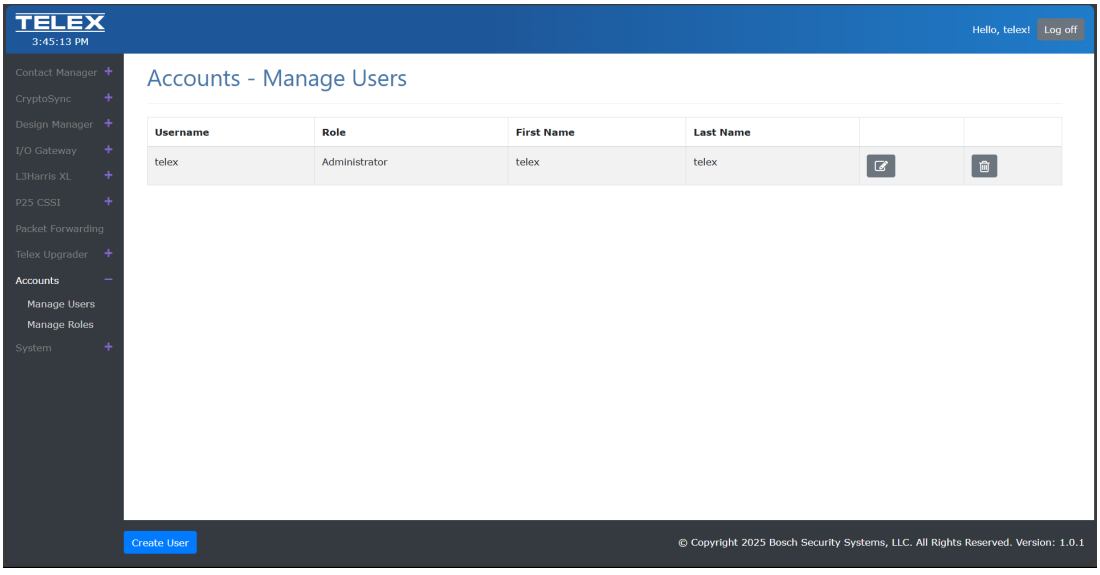
Notice!
We recommend that you create multiple users. Do not solely use the default administrator account.

7.1 Manage Users

As an administrator to the CMS system, you can add or edit users in the system.

To **access the Manage Users screen**, do the following:

- From the left navigation, click **Accounts | Manage Users**.
  The Manage Users screen appears.



Username Column
The **Username** column displays the all the usernames in the system.

Role Column
The **Role** column displays the role assignment for the user.

Notice!
Create roles shown in this field on the Manage Roles screen. For more information, see *Manage Roles, page 24*.

First Name Column
The **First Name** column displays the first name of the user.

Last Name Column
The **Last Name** column displays the last name of the user.

Edit Button

The **Edit** button opens the Manage User screen for the user selected. From here, you can make modifications to the user profile.

Delete Button

The **Delete** button deletes the selected user profile.

Caution!

No message confirmation for deletion

Once you click the delete button, the selected item is deleted. If you delete the item by mistake, you must create a new item.

Create User Button

The **Create User** button opens the Create User screen. For more information, see *Create Users, page 21*.

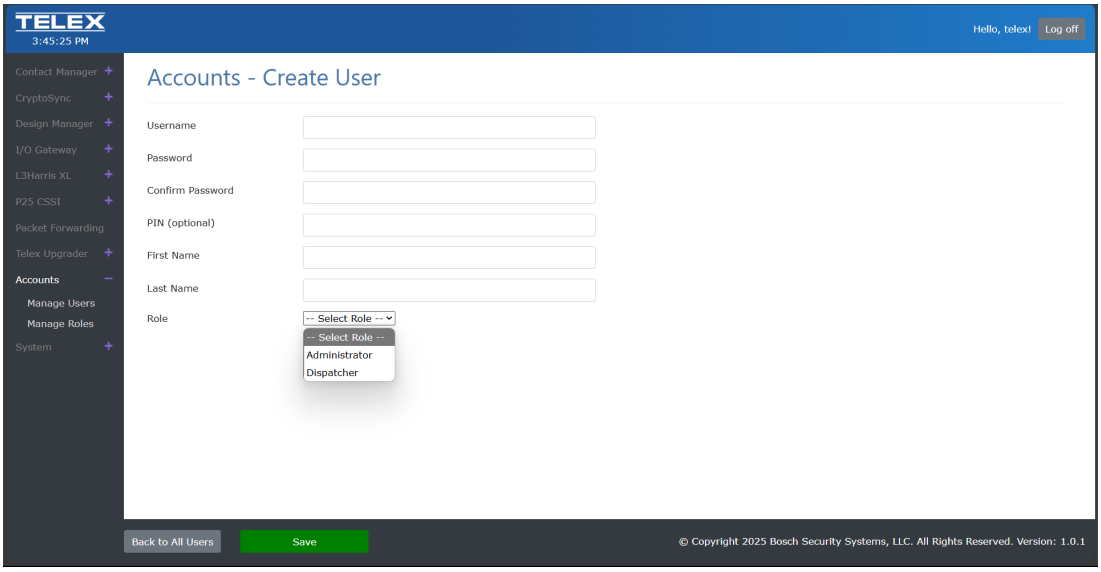
To edit a user profile, see *Edit Users, page 22*.

7.1.1 Create Users

Use the **Create Users** screen to create users in the CMS system.

To **access the Create Users screen**, do the following:

- On the Manage Users screen, click **Create User**.
  The Create User screen opens.



Username Field

Use the **Username** field to view, create, and modify the username of the current profile.

Usernames must start with a letter and cannot include special characters other than '_' and '-'.

Password Field

Use the **Password** field to view, create, or modify the current password as asterisks.

Passwords must include a capital letter, a lowercase letter, a number, and a special character.

Confirm Password

Use the **Confirm Password** field to retype exactly the password for the user profile which is necessary when changing the user profile's password.

PIN (optional) Field

Use the **PIN (optional)** field to add an extra level of security to your login.

PINs must be at least 5 digits up to a maximum of 64 digits.

First Name Field

Use the **First Name** field to enter or modify the first name of the user.

Last Name Field

Use the **Last Name** field to enter or modify the last name of the user.

Role Drop Down Menu

Use the **Role** drop down menu to select the role assignment for this user.

Notice!

Create roles shown in this field on the Manage Roles screen. For more information, see *Manage Roles, page 24*.

Save Button

Click the **Save** button to save the user profile and any modifications made.

Back to All Users Button

Click the **Back to All Users** button to return to the Manage Users screen.

Notice!

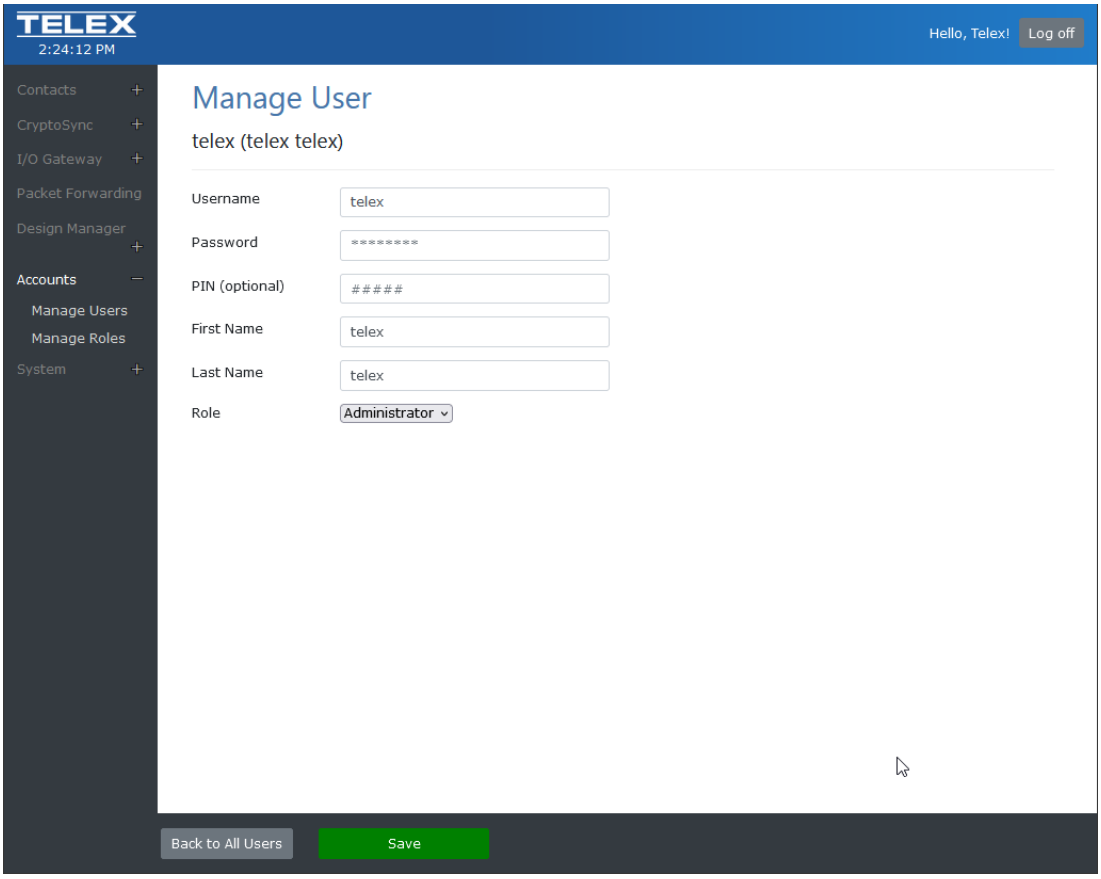
If you make modifications to the profile, and then click the Back to All Users button without saving, the modifications you make are discarded. Be sure to click Save after making any changes.

To **create a user profile**, do the following:

1. Enter a **username**.
2. Enter a **password**.
3. Re-type the **password exactly**.
4. (optional) Enter a **PIN**.
5. Enter the **first name** of the user.
6. Enter the **last name** of the user.
7. Select a **role** to assign.
8. Click **Save**.
9. Click **Back to All Users**.
   The Manage Users screen appears.
10. Verify the **new user profile** appears.

7.1.2 Edit Users

Use the Manage User screen to modify and change a user profile.



Username Field

Use the **Username** field to set the username of the user profile.

Usernames must start with a letter and cannot include special characters other than '_' and '-'.

Password Field

Use the **Password** field to set the password of the user profile.

Passwords must include a capital letter, a lowercase letter, a number, and a special character.

PIN (optional) Field

Use the **PIN (optional)** field to add an extra level of security to your login.

PINs must be at least 5 digits up to a maximum of 64 digits.

First Name Field

Use the **First Name** field to enter or modify the first name of the user.

Last Name Field

Use the **Last Name** field to enter or modify the last name of the user.

Role Drop Down Menu

Use the **Role** drop down menu to select the role assignment for this user.

Save Button

Click the **Save** button to save the user profile and any modifications made.

Back to All Users Button

Click the **Back to All Users** button to return to the Manage Users screen.

Notice!

If you make modifications to the profile, and then click the Back to All Users button without saving, the modifications you make are discarded. Be sure to click Save after making any changes.

To **edit a user profile**, do the following:

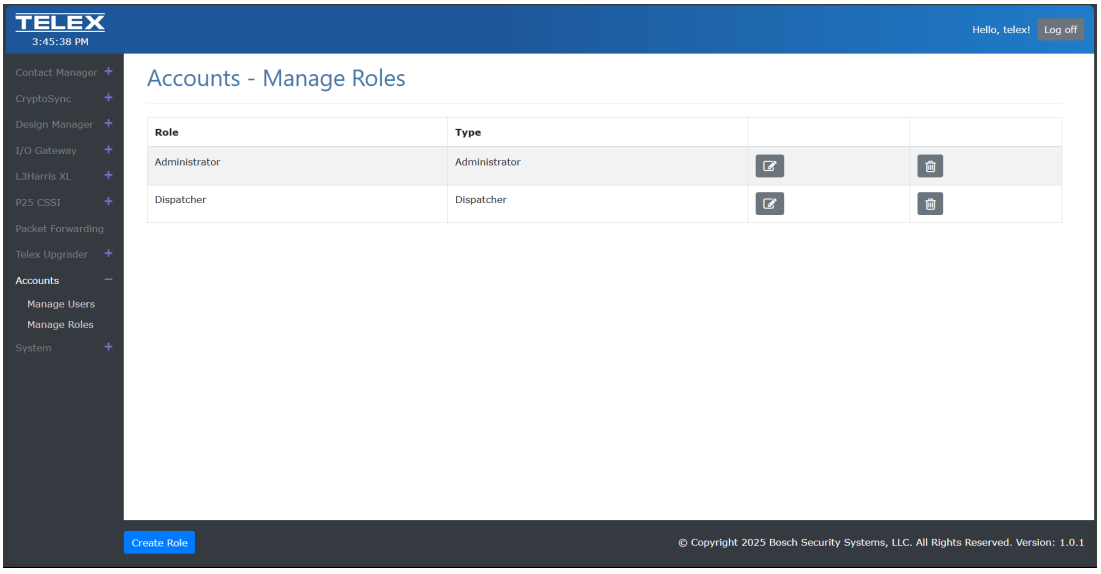
1. From the left navigation, click **Accounts | Manage Users**.
   The Manage Users screen opens.
2. Select a **username** from the list.
3. Click the **Edit icon**.
   The Manage User screen opens.
4. Make the **necessary changes**.
5. Click **Save**.

7.2 Manage Roles

Use the Manage Roles screen to create, maintain and delete the different roles that are assigned to users.

To **access the Manage Roles screen**, do the following:

- From the left navigation bar, click **Accounts | Manage Roles**.
  The Manage Roles screen appears.



Role Column

The **Role** column displays a list of roles in the CMS system.

Type Column

The **Type** column displays the type of role.

Edit Button

The **Edit** button opens the Create Role screen. You can make modifications in this screen.
For more information, see Create Role.

Delete Button

The **Delete** button deletes the selected Role.

Caution!

No message confirmation for deletion

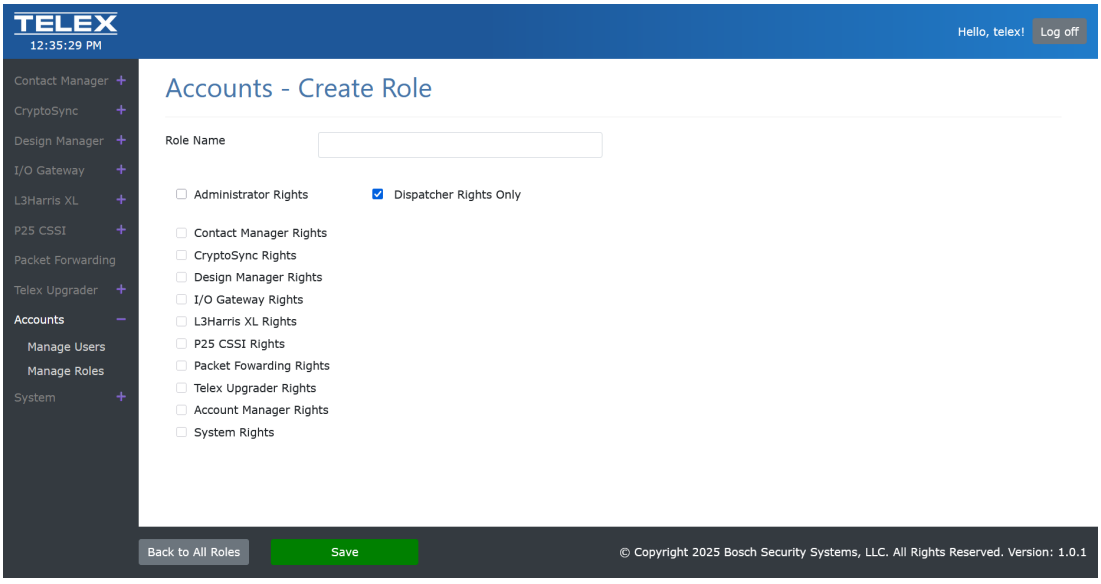
Once you click the delete button, the selected item is deleted. If you delete the item by mistake, you must create a new item.

Create Role Button

The **Create Role** button opens the Create Role screen.

7.2.1 Create Role

Use the **Create Role** screen to create different assignable roles that dictates the amount of access a user has in the system.



Role Name Field

Use the **Role Name** field to enter the name of the role you want to create.

Administrator Rights Check Box

The **Administrator Rights** check box enables administrator rights for the role. Administrators have access to all areas of the system.

Dispatcher Rights Only Check Box

The **Dispatcher Rights Only** check box enables dispatcher rights only for the role.

Contact Management Rights Check Box

The **Contact Management Rights** check box enables contact management rights to the role.

CryptoSync Rights Check Box

The **CryptoSync Rights** check box enables CryptoSync rights to the role.

Design Manager Rights Check Box

The **Design Manager Rights** check box enables Design manager rights to the role.

I/O Gateway Rights Check Box

The **I/O Gateway Rights** check box enables I/O gateway rights to the role.

L3Harris XL Rights Check Box

The **L3Harris XL Rights** check box enables L3Harris XL rights to the role.

P25 CSSI Rights Check Box

The **P25 CSSI Rights** check box enables P25 CSSI rights to the role.

Packet Forwarding Rights Check Box

The **Packet-Forwarding Rights** check box enables packet-forwarding rights to the role.

Telex Upgrader Rights Check Box

The **Telex Upgrader Rights** check box enables the ability to use the Telex Upgrader option.

Account Manager Rights Check Box

The **Account Manager Rights** check box enables Account manager rights. Without this option the users in this role have no access to the manage users or manage roles pages.

System Rights Check Box

The **System Rights** check box enables System Rights. Without this option the users in this role cannot access items such as logs, SSL settings, or factory reset options for the device.

To **create a Role**, do the following:

1. Navigate to **Accounts | Manage Roles**.
   The Manage Roles screen appears.
2. Click the **Create Role button** at the bottom of the screen.
   The Create Role screen appears.
3. Enter a **Role Name**.
4. Select the **check boxes** for the rights to assign to this role.
5. Click **Save**.

8 System Management Operation

Use the **System Management Page** to open the System Status and Management screen, as well as view active client connections.

8.1 System Status and Management

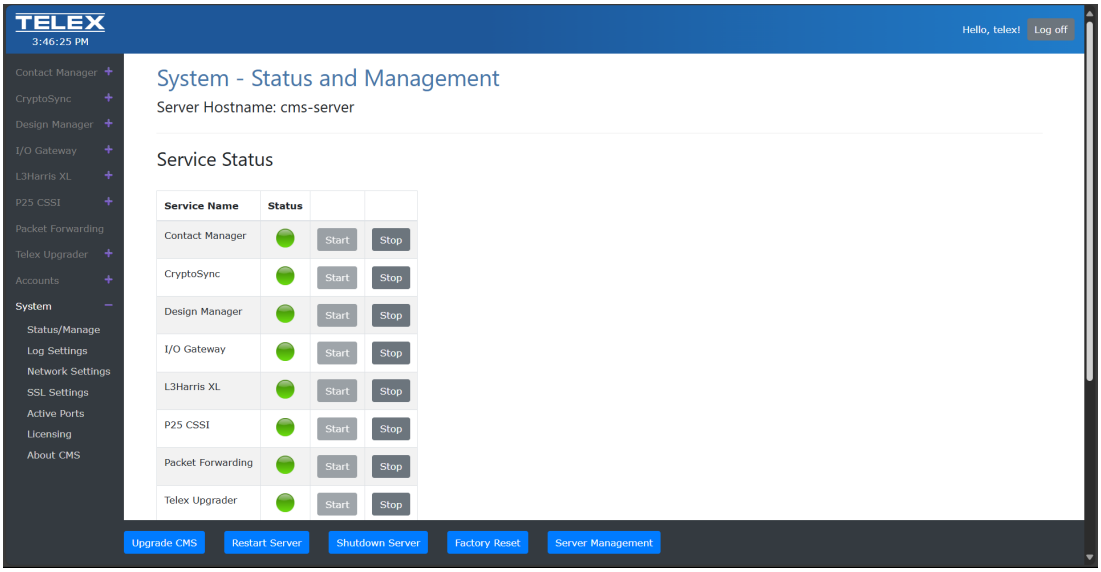
Use the **System Status and Management** page to monitor, maintain, start, and stop services in the system.

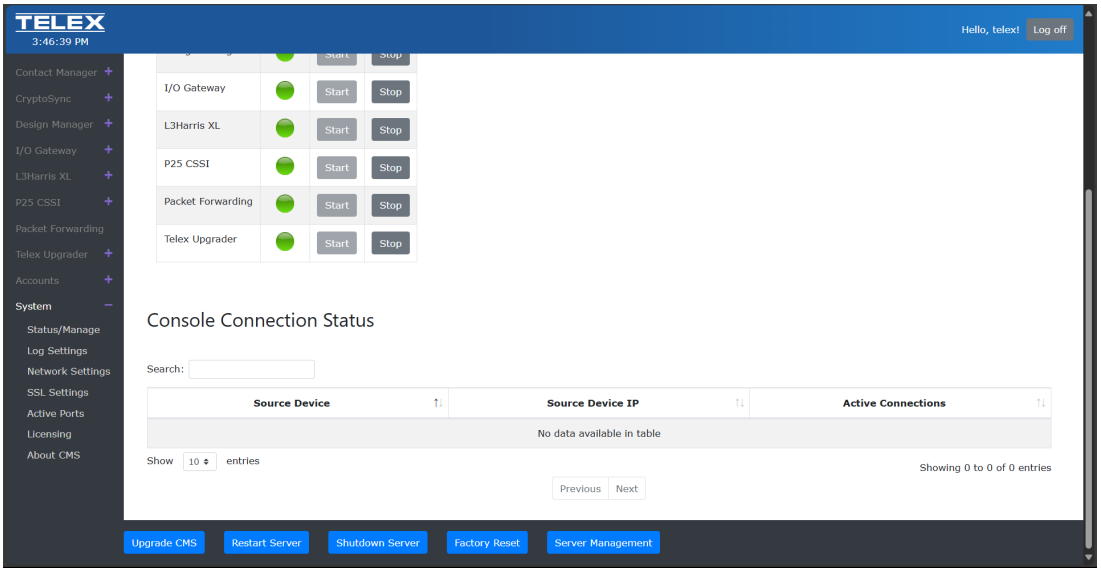
8.1.1 Service Status

Available Management services:

- Contact Management
- CryptoSync
- I/O Gateway
- Packet Forwarding
- Design Manager

In addition, Server Restart, Server Shutdown, and Server Management are possible from this page. You can also perform a factory reset from this page.





To **start or stop a service**, do the following:

- Press the **start button** to start a stopped service.
  OR
  Press the **stop button** to stop the individual service.

8.1.2 Console Connection Status

The Console Connection Status consists of three columns:

- Source Device displays the connected device's name. This corresponds to a C-Soft position's 'Position Name' setting, and is used for easy identification of the device.
- Source Device IP displays the connected device's IP address.
- Active Connections displays which CMS module(s) that device is currently connected to. Currently, the list only supports active state information for Contact, Design, and CryptoSync modules.

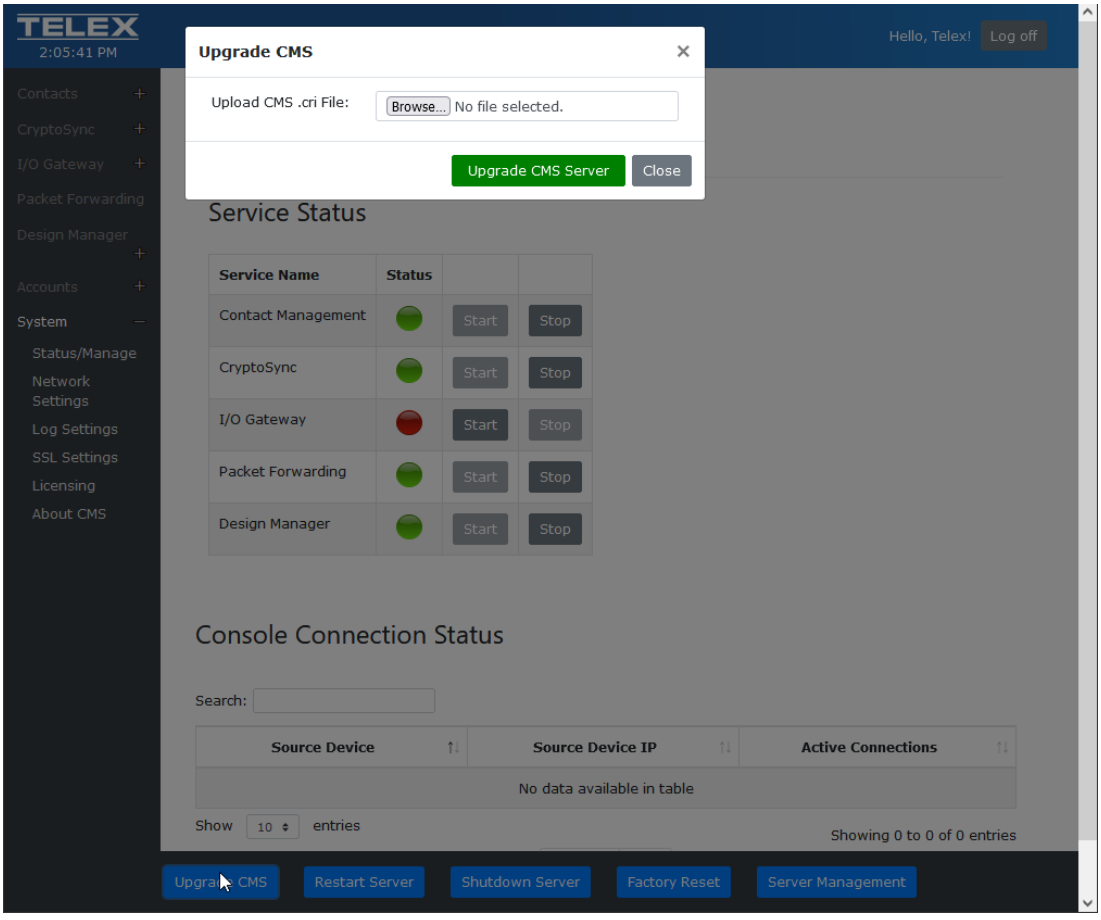
8.1.3 Upgrade CMS

When a new CMS version is released, it may be desirable to upgrade the Console Management Server software to a new version to gain access to new features and new bug fixes.

Notice!
Please read all release notes before upgrading your CMS to check for any compatibility issues. Contact Telex technical support for additional information.

To **upgrade CMS**, do the following:

1. Click **Upgrade CMS** on the System Status and Management page.
   The Upgrade CMS window opens.

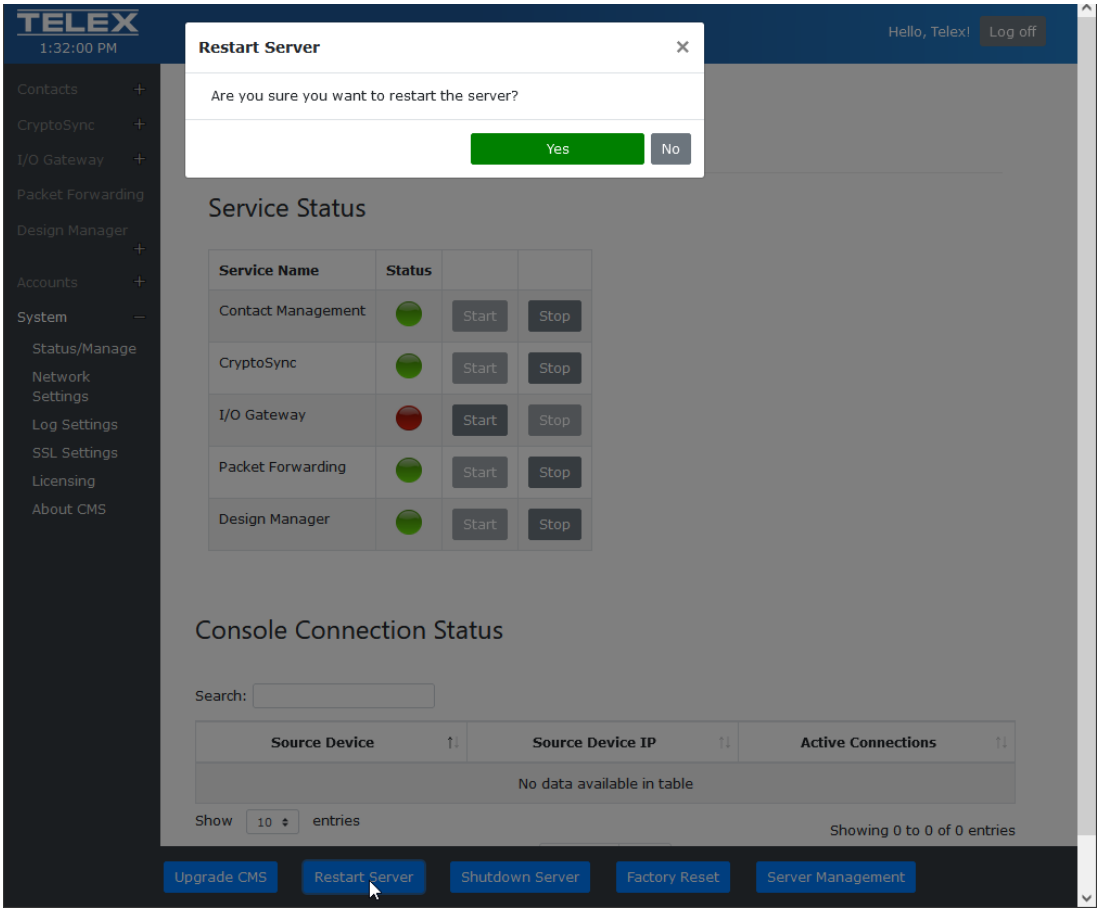


2. Click **Browse...**.
3. Navigate to the **.cri file** to upload to the system.
4. Click **Upgrade CMS Server**.
   The .cri file uploads to the system. Once the file uploads, the updates are applied and the web server and all services are restarted.

8.1.4 Restart Server

To **restart the entire CMS server**, do the following:

1. Click **Restart Server**.
   A Restart Server confirmation message appears.

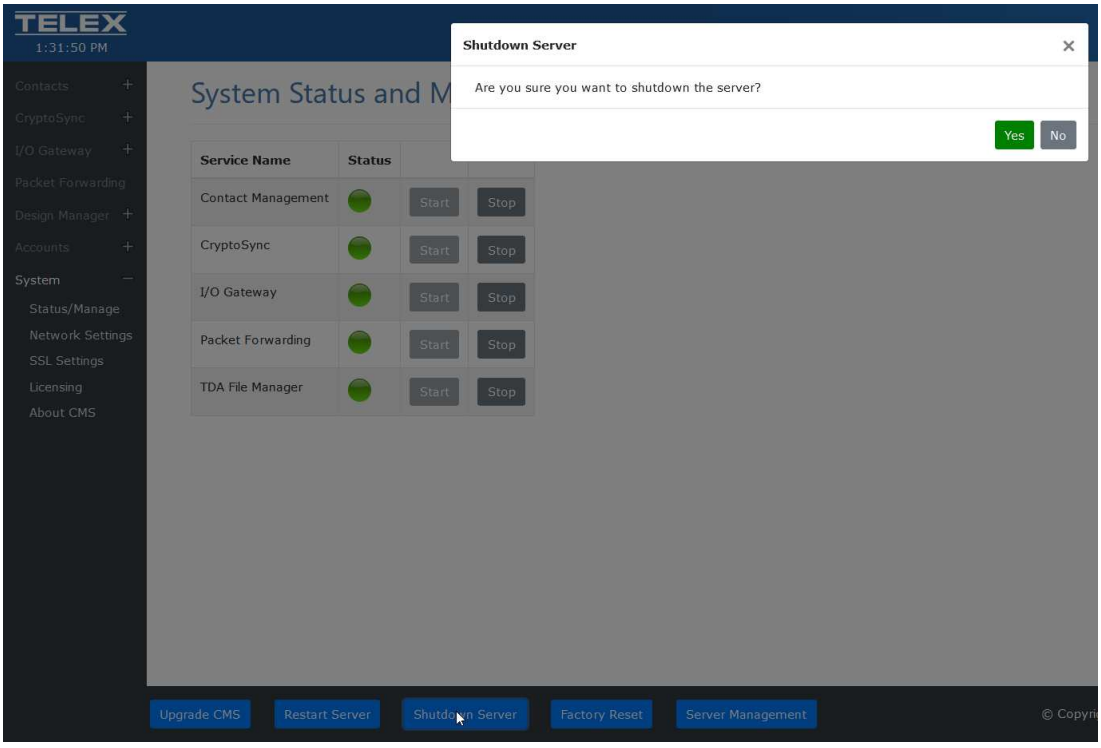


2. Click **Yes**.

8.1.5 Shutdown Server

To **shut down the server**, do the following:

1. Click **Shutdown Server**.
   A shutdown the server confirmation message appears.



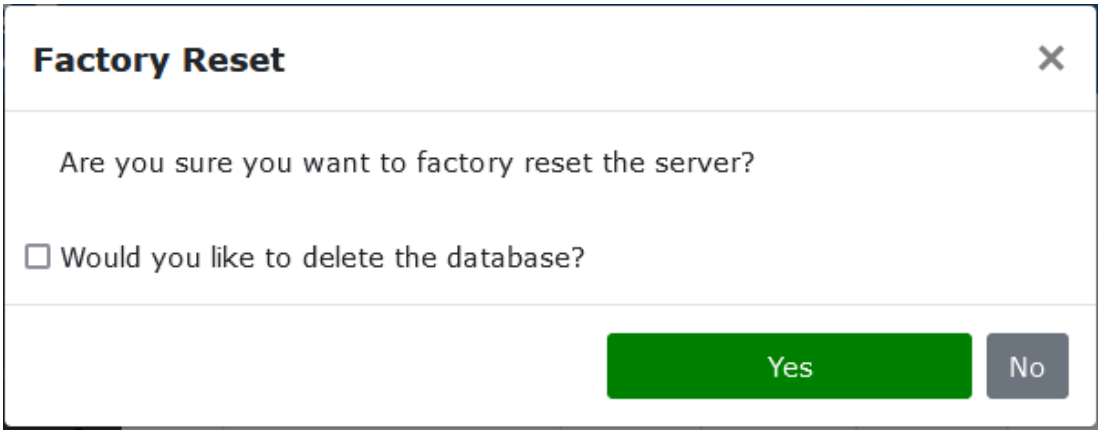
2. Click **Yes**.
   The entire CMS server is shut down.

8.1.6 Factory Reset

Use **Factory Reset** to revert the server to its factory default settings. The IP Address resets to 169.254.x.x. The user has the option to keep or remove the current database.

To **perform a factory reset**, do the following:

1. Click **Factory Reset**.
   A confirmation message appears.



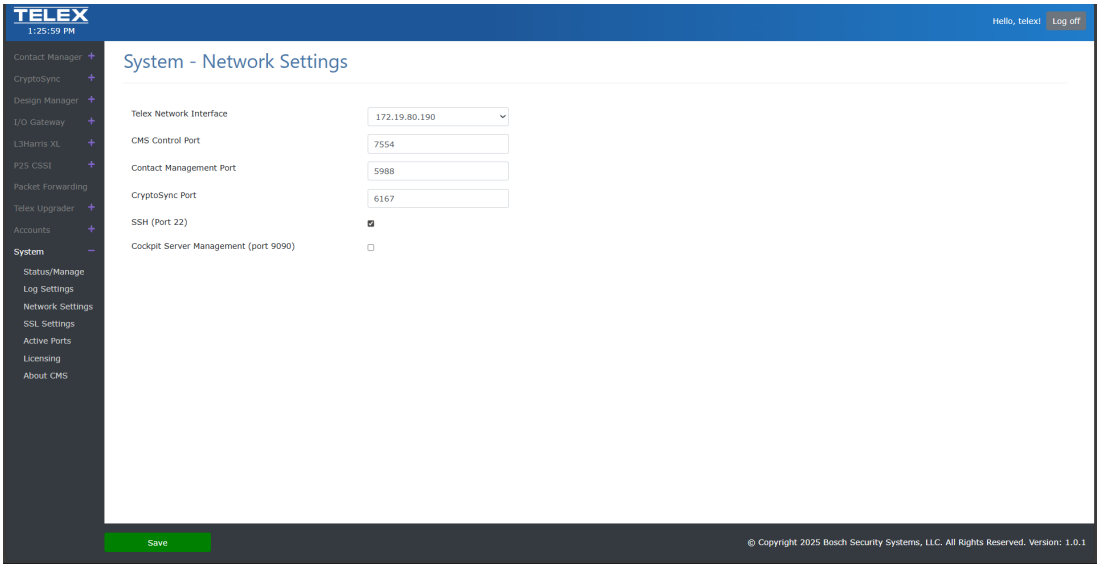
2. Select the **Would you like to delete the database check box**, if applicable.
3. Click **Yes**.
   The Server resets to its factory default settings.

8.1.7 Server Management

8.2 Network Settings

Use the **Network Settings** page to set the Control Port, Alias Management Port, and the CryptoSync Port.

Notice!
When a service port is changed, the service restarts and the port is opened in the firewall automatically.



Telex Network Interface Drop Down Menu
Use the **Telex Network Interface** drop down menu to select the Ethernet port for CMS communication. All programmed IP addresses appear in the list.

CMS Control Port Field
Use the **CMS Control Port** field to enter the port used to communicate with CMS clients. This port value must be specified in the Console Configuration Tool's Control Port and in IP-224's Control Port for SRTP Encryption.

Contact Management Port Field
Use the **Contact Management Port** field to enter the port used for contact management.

CryptoSync Port Field
Use the **CryptoSync Port** field to enter the port used for CryptoSync communication.

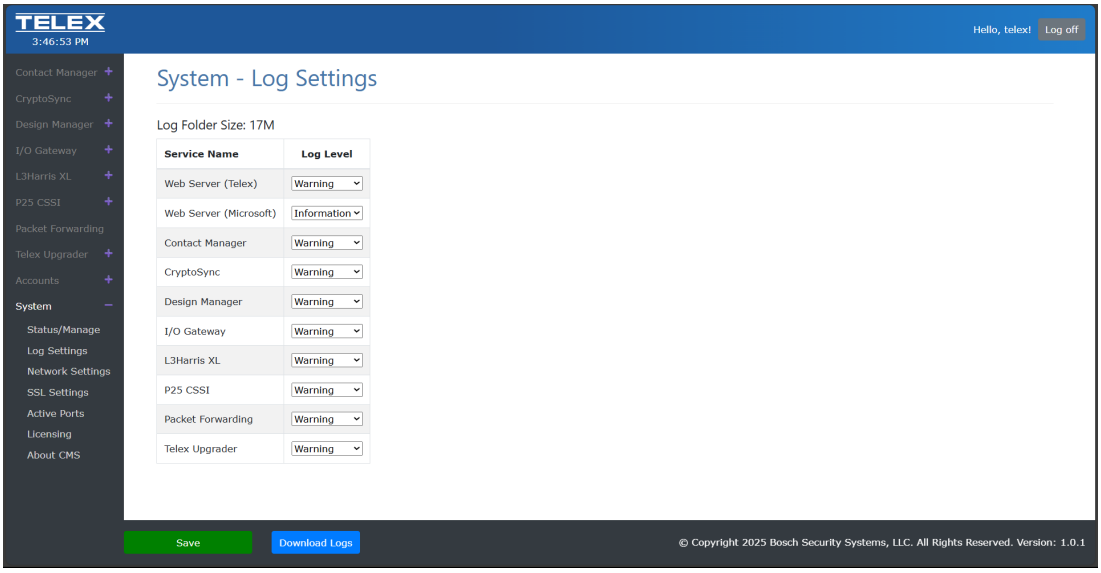
Notice!
The SSH and Cockpit Management features are intended for Linux system administrators to manage the CMS hardware. These tools allow administrators to access the device, monitor performance, and perform administrative tasks.

Telex does not recommend enabling these options due to potential security risks.

8.3 Log Settings

Use the **Log Settings** page to select a log level to specify the amount of information stored in each service's log files. Log files are computer generated data files that contain information about usage, activities, and operations within the system.
CMS can create log files for seven different services: Web Server (Telex), Web Server (Microsoft), Contact Management, CryptoSync, I/O Gateway, Packet Forwarding, and Design Manager.
Five log levels available that trigger the system to create a log file: Debug, Information, Warning, Error, Fatal.
To **configure the Log Settings page**, do the following:

1. Navigate to **System | Log Settings** in the left navigation.
   The System Log Settings page opens.



2. Select the **log level** from the Log Level drop down menu for the service.
3. Repeat **step 2** until all the services have been configured.
4. Click the **Save button**.

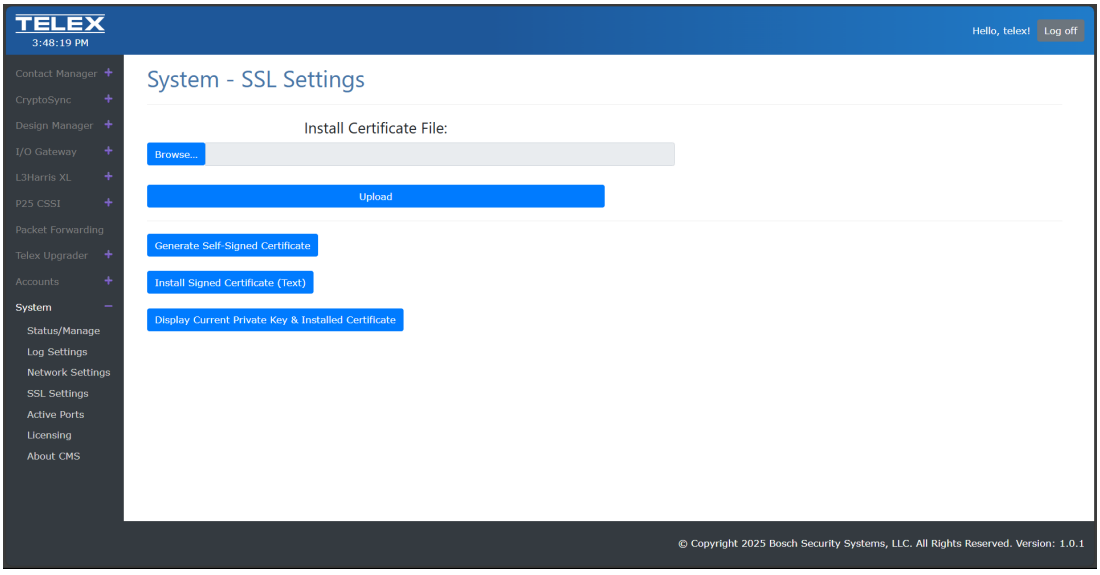
Download Logs

Use the **Download Logs** button to produce a text file of the log files for the different services. Depending on the size of the file, a .zip file may be used to deliver the files. Use any simple word editor, such as Notepad, to view the files.
To **download log files**, do the following:

- Click the **Download Logs button** at the bottom of the page.
  A .txt or .zip file appears depending on the size of the file.

8.4 SSL Certificate

Use the **SSL Certificate** page to allow users to install their custom SSL Certificate for the CMS web server. An SSL Certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. CMS uses SSL certificates generated by a third party application called openssl.



There are two ways to load SSL certificates:

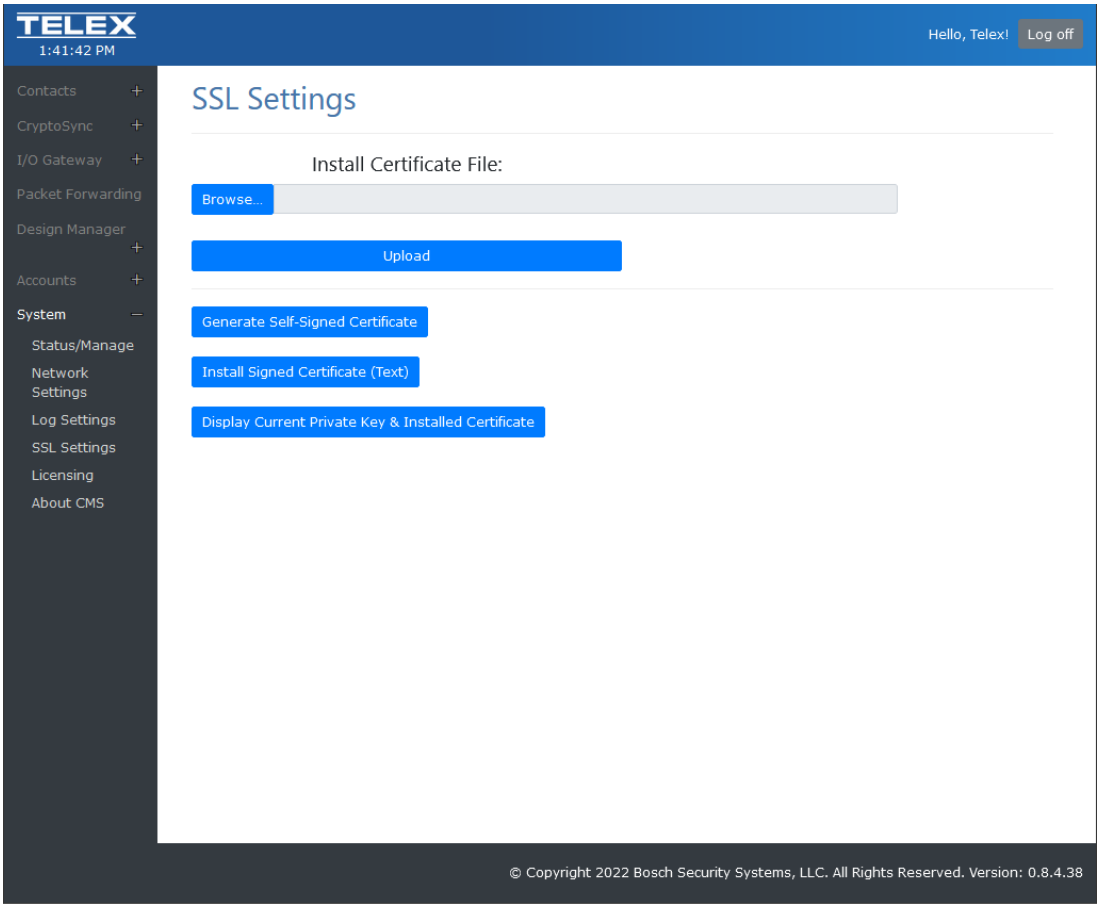
– Manually install a certificate file
– Generate self-signed certificate

8.4.1 Install a SSL certificate file manually

If you have an SSL certificate already, you can upload it to CMS.

To **install a certificate file manually**, do the following:

1. Click **System | SSL Settings page**.
2. Click **Browse**.

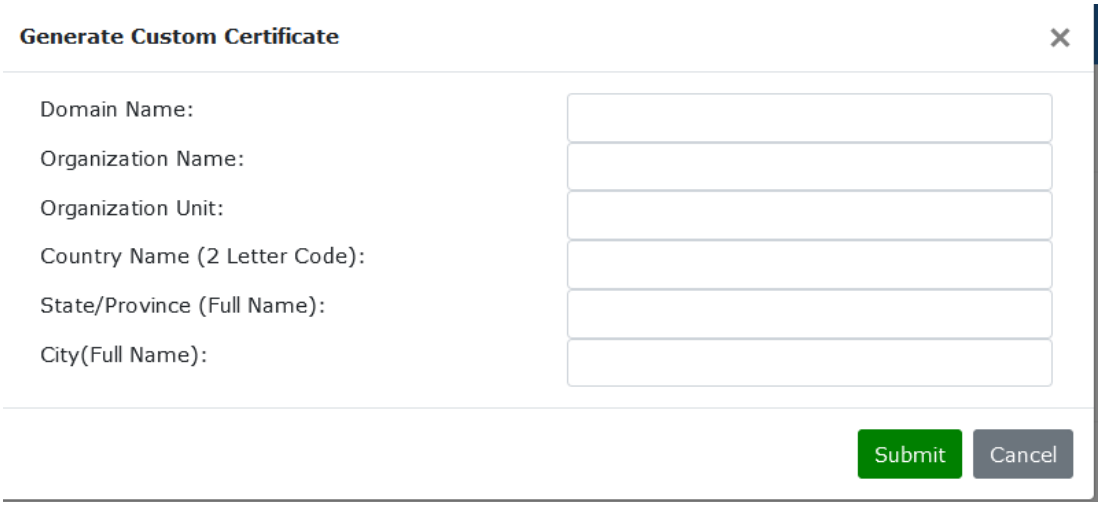


3. Navigate to the **SSL certificate file** you want to use.
4. Click **Open**.
5. Click **Upload**.

8.4.2 Generate a custom SSL certificate using CMS

To **generate a custom SSL certificate**, do the following:

1. Click **System | SSL Settings**.
2. Click **Generate Self-Signed Certificate**.
   The Generate Custom Certificate screen opens.



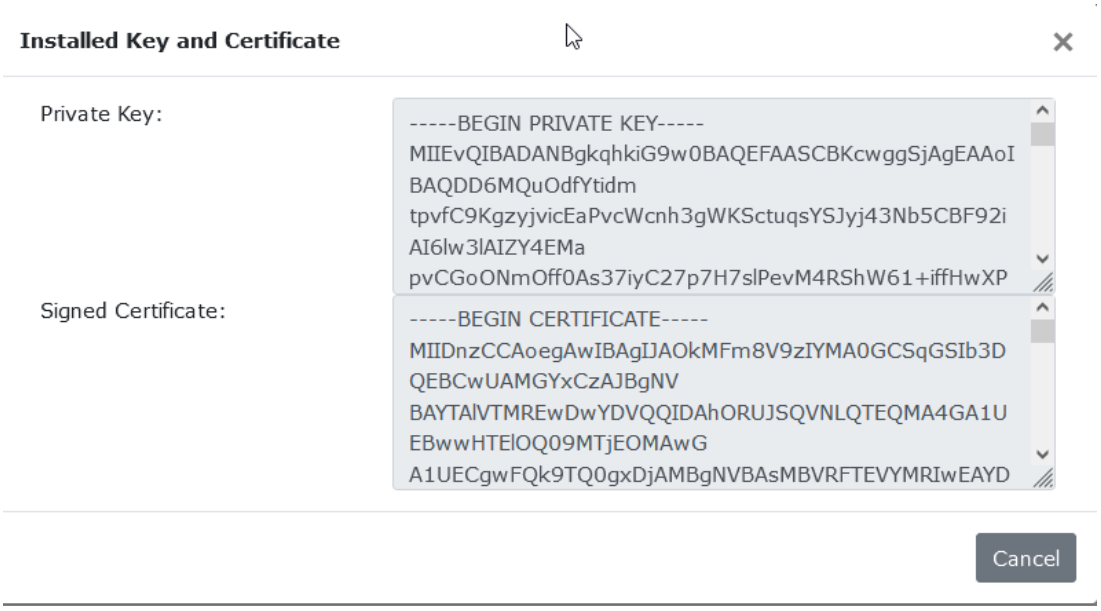
3. Enter the following information:
   - Enter the **Domain Name**. This is the IP address of the CMS Server.
   - Enter the **Organization Name**.
   - Enter the **Organization Unit**.
   - Enter the **two character country name** (for example, US).
   - Enter the **State/Province**.
   - Enter the **City**.
4. Click **Submit**.
   The Custom Key and Certificate screen opens with a private key and a signed certificate generated.
5. Copy the **Private Key** and save into a text file.
6. Copy the **Certificate Authority (CA) Signed Certificate** and save into a text file.
7. Click **Cancel**.
   The Custom Key and Certificate screen closes.
8. Click **Install Signed Certificate**.
   The Install Certificate Authority (CA) Certificate screen appears.

9. Copy and paste the **Private Key** from the test file to the Private Key field.
10. Copy and paste the **Certificate Authority (CA) Signed Certificate** from the text file to the Certificate Authority (CA) Signed Certificate field.
11. Click **Submit**.
    CMS installs the customer certificate and restarts.

8.4.3 Display the current installed Private Key and Installed Certificate

To **display the current installed Private Key and Certificate**, do the following

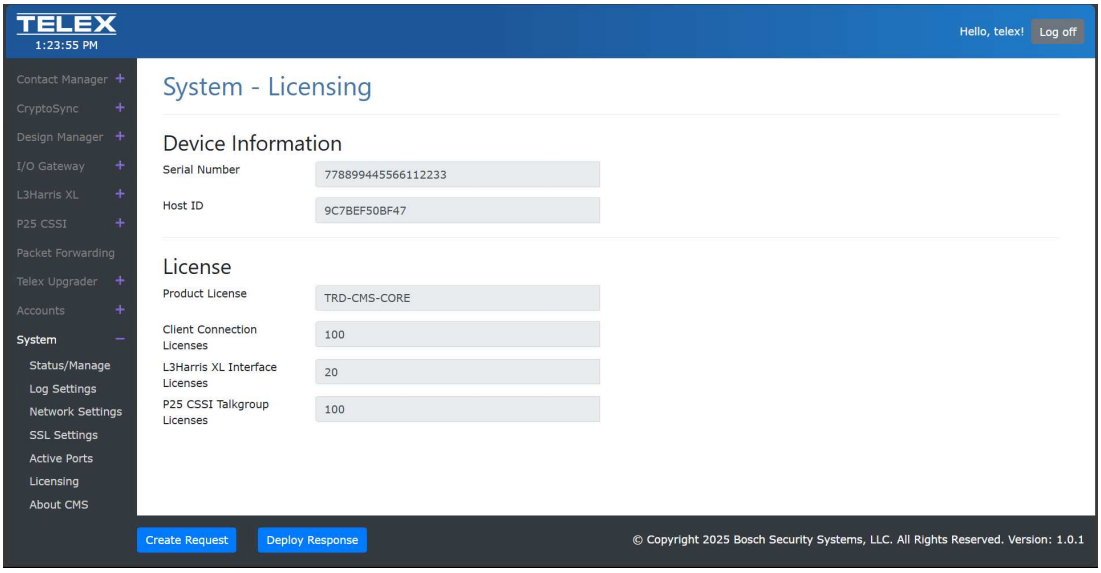
1. Click **System | SSL Certificates**.
2. Click **Display Private Key, Installed Certificate**.
   The Installed Key and Certificate screen opens with the current private key and certificate fields populated.



8.5 Licensing

Use the **Licensing** page displays the CMS licensing information. This information includes the device's serial number and host ID, which is needed for Telex license management and license deployment. The License page also provides access to two licensing operations needed for license deployment:

– Create capability request
– Process capability response

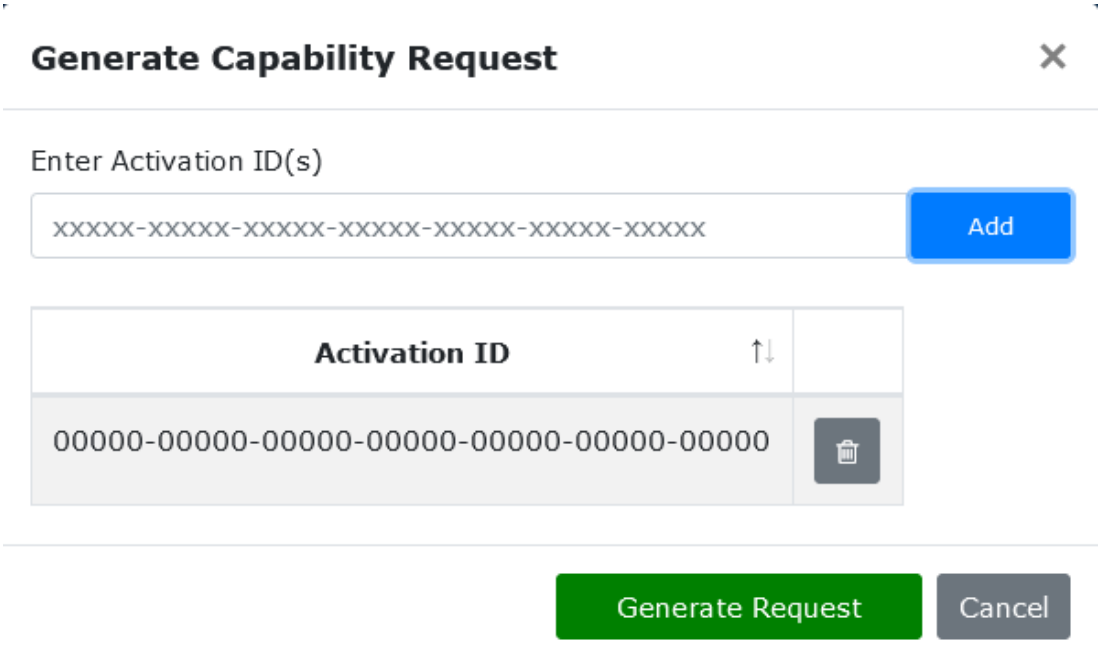


8.5.1 Create a capability request

Upon purchase of a new license and receipt of an Activation ID, it is necessary to first generate a capability request.

To **create a capability request**, do the following:

1. Select **System | Licensing**.
2. At the bottom of the page, click **Create Request**.
   Generate Capability Request screen opens.



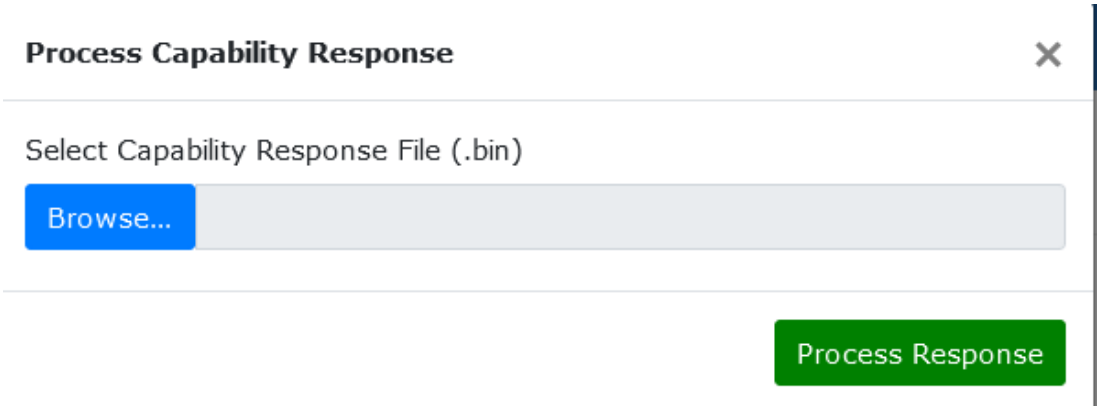
3. Enter the **Activation ID**.
4. Click the **Add button**.
5. Repeat **steps 3 and 4**, as needed.
6. When finished, click **Generate Request**.
   The request is generated.
7. Click **Save** to save the request.

8.5.2 Deploy a capability response

After processing a capability request, it is necessary to deploy the capability response file to the device.

To **deploy a capability response**, do the following:

1. Click **System | Licensing**.
2. At the bottom of the window, click the **Deploy Response button**.
   The Process Capability Response screen opens.



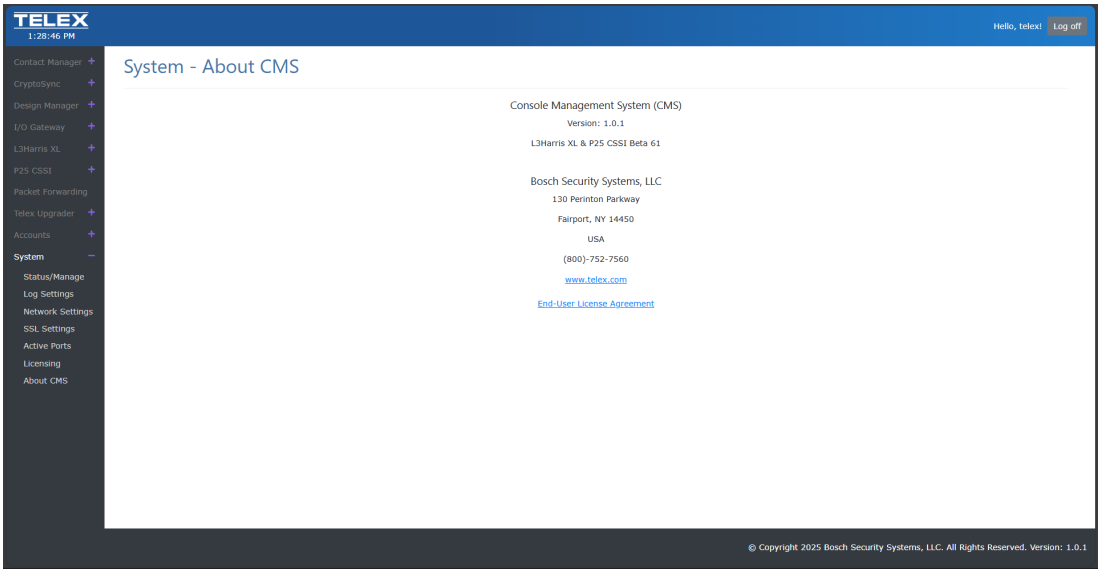
3. Click the **Browse... button**.
4. Select the **capability response file**.
5. Click the **Process Response button**.

The licensing page refreshes and displays the newly activated license. It may be necessary to start or restart various services to ensure the newest license capabilities are applied. For more information, see *System Status and Management, page 27*.

8.6 About CMS

The **About CMS** screen shows the current version of the CMS installation and the contact information for Bosch Security Systems, LLC.

You can also access the EULA (End User License Agreement) from this page.


TELEX
1:28:46 PM
Hello, telex!
Log off
Contact Manager
CryptoSync
Design Manager
I/O Gateway
L3Harris XL
P25 CSSI
Packet Forwarding
Telex Upgrader
Accounts
System
Status/Manage
Log Settings
Network Settings
SSL Settings
Active Ports
Licensing
About CMS
System - About CMS
Console Management System (CMS)
Version: 1.0.1
L3Harris XL & P25 CSSI Beta 61
Bosch Security Systems, LLC
130 Perinton Parkway
Fairport, NY 14450
USA
(800)-752-7560
www.telex.com
End-User License Agreement
© Copyright 2025 Bosch Security Systems, LLC. All Rights Reserved. Version: 1.0.1

9 Design Manager Configuration and Operation

9.1 User/Role Creation

Design management utilizes the same username and password as the CMS web software. For more information, see *Account Management, page 20*.
For simplicity, it is recommended to create a Dispatchers role and assign user accounts the Dispatcher role.

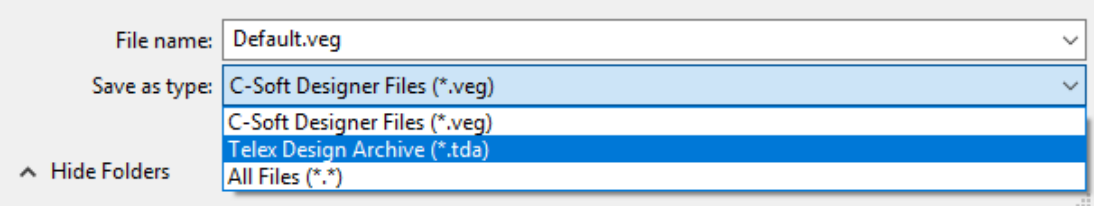
Notice!
For the purpose of TDA management, user roles do not need to have special permissions.

9.2 CMS Design Repository

9.2.1 Create TDA Files

The Design Manager requires all designs saved in the TDA file format for portability.
To **convert existing designs**, do the following:

1. Launch **C-Soft Designer**.
2. Open an **existing design (.veg) file**.
3. Select **File | Save As**.
   The Save As screen opens.

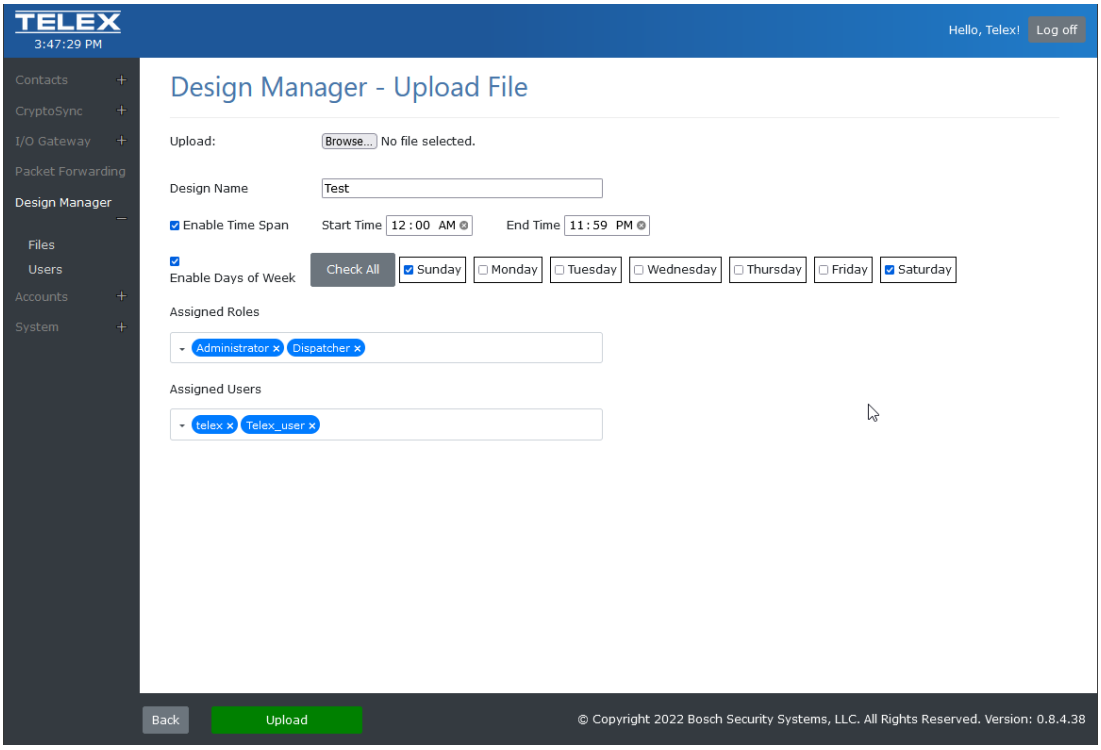


4. From the Save As type drop down menu, select **Telex Design Archive (*.tda)**.

9.2.2 Upload Designs

For a design to be available for distribution to clients using the Design Manager, the design needs to reside to the CMS Design Repository.
To **upload a design to the CMS Design Repository**, do the following:

1. Select **Design Manager**.
2. Click **the Upload File button** at the bottom of the screen.
   The Design Manager - Upload File screen opens.



3. Click the **Browse... button**.
   An explorer window opens.
4. Select a **Telex Design Archive (.tda) file**.
5. Click **Open**.
6. Enter a **Design Name** for the design.
   Use an easily identifiable name for the file.

Optional

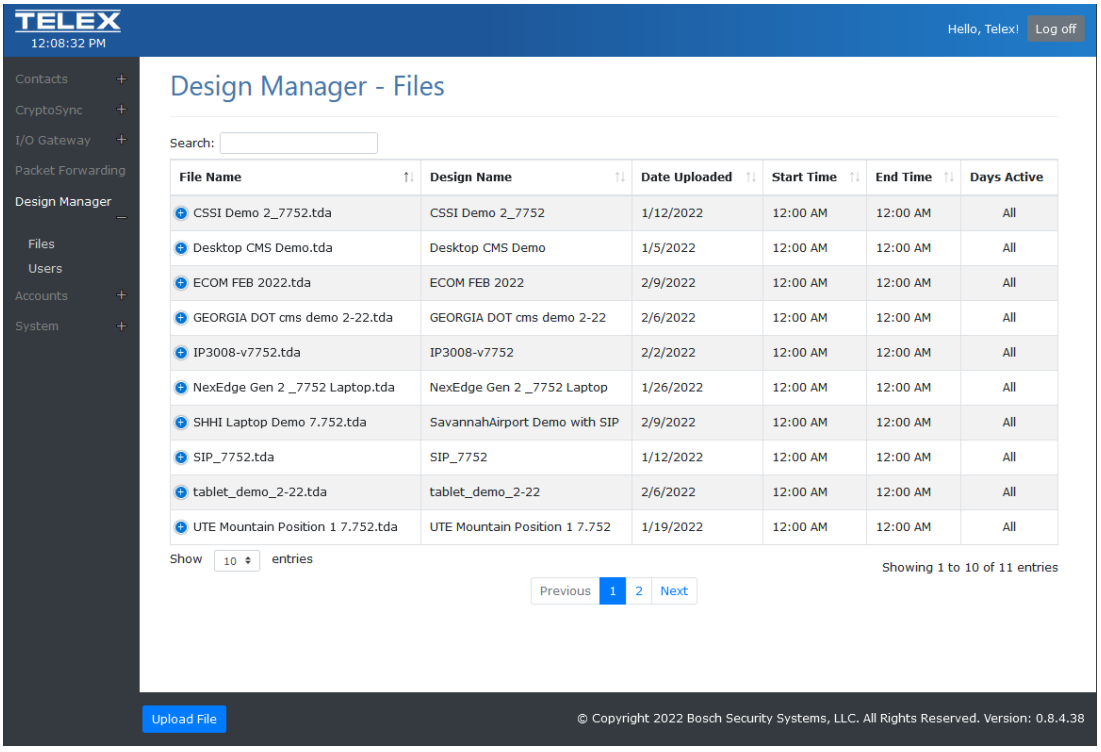
1. Select the **Enable Time Span check box** to specify a start and end time of day for when this is design is to be accessible.
   This field is useful for specifying design availability on a shift-based schedule.
2. Select the **Enable Days of Week check box** to specify which days of the week that this design is to be accessible.
   This field is useful for specifying design availability on a shift-based schedule.
3. Select the **roles** to provide access to the design.
4. Select the **users** to provide access to the design.
5. When finished, click the **Upload button**

9.2.3 Manage Uploaded Designs

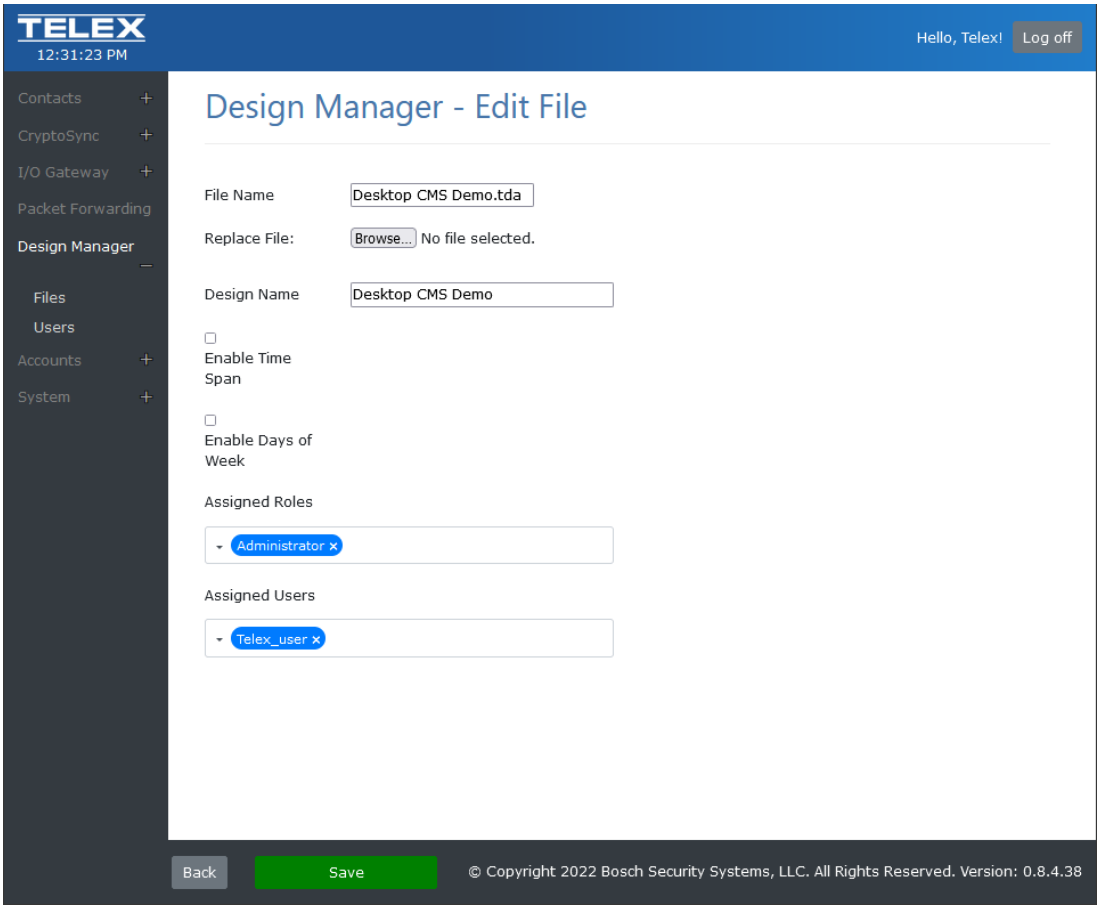
After uploading designs to the Design repository, use the Files page to manage the design repository. Use the Files page to upload a new version of a design, edit accessibility parameters, or download a design.

To **manage designs**, do the following:

1. Click **Design Manager**.
2. Click **Files** to view the list of designs.



3. Click the **Edit icon** to make changes to an existing design.
   This includes uploading a new version of the design, changing the design name, and altering accessibility parameters.



4. Click the **Delete icon** to remove the design from the design repository.

5. Click the **Download icon** to download the design.

9.3 C-Soft/CMS Connection Configuration

Use the Console Configuration Tool to configure and manage each C-Soft instance to connect and use CMS as a position-based setting.

Console Management System Page

Use the **Console Management System Page** to configure the communication address and port.

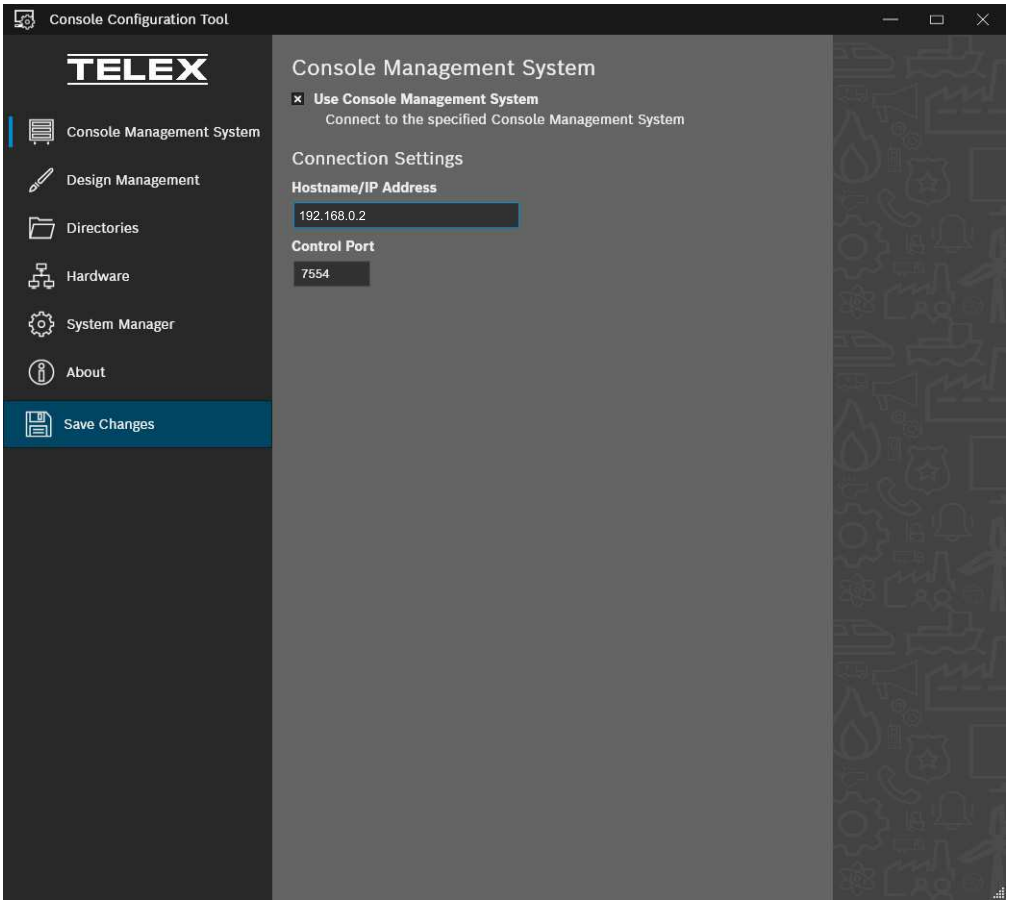


Figure 9.1: Console Configuration Tool | Console Management System Page

Use Console Management System Check Box

The **Console Management System** check box signals that the dispatch position should connect to CMS.

Hostname/IP Address Field

Use the **Hostname/IP Address** field to enter the hostname or IP address of CMS.

Control Port Field

Use the **Control Port** field to enter CMS' Control Port setting.

Design Management Page

Use the **Design Management Page** to configure C-Soft's behavior in determining which design to launch on startup.

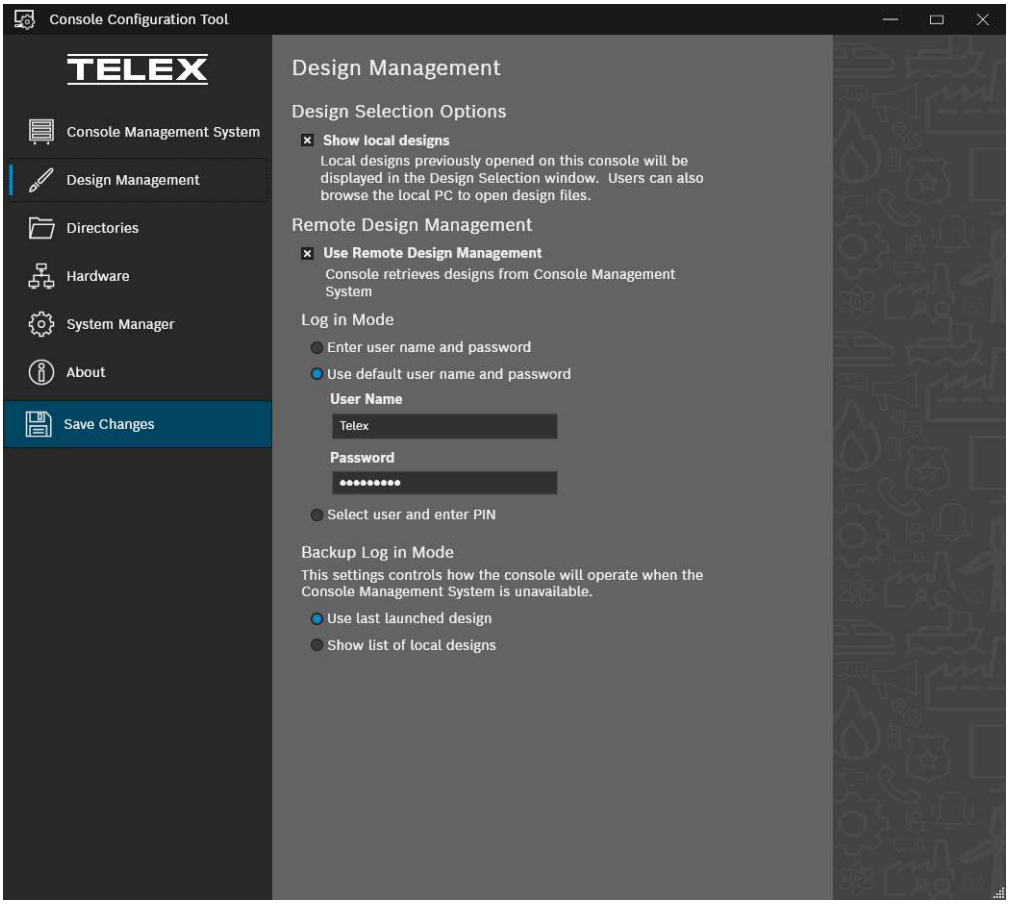


Figure 9.2: Console Configuration Tool | Design Management Page

Show local designs Check Box

Use the **Show local designs** check box to show a list of recently opened designs when C-Soft launches.

Use Remote Design Management Check Box

The **Use Remote Design Management** check box indicates whether C-Soft should attempt to utilize CMS's Design Management feature. If selected, the Log in Mode radio buttons become active.

Log in Mode

The **Log in Mode** radio buttons determine how the user accesses CMS when C-Soft launches.

- Select the **Enter user name and password radio button** to require a user name and password every log in attempt.
- Select the **Use default user name and password radio** button to automatically login using the provided credentials.

Backup Log in Mode

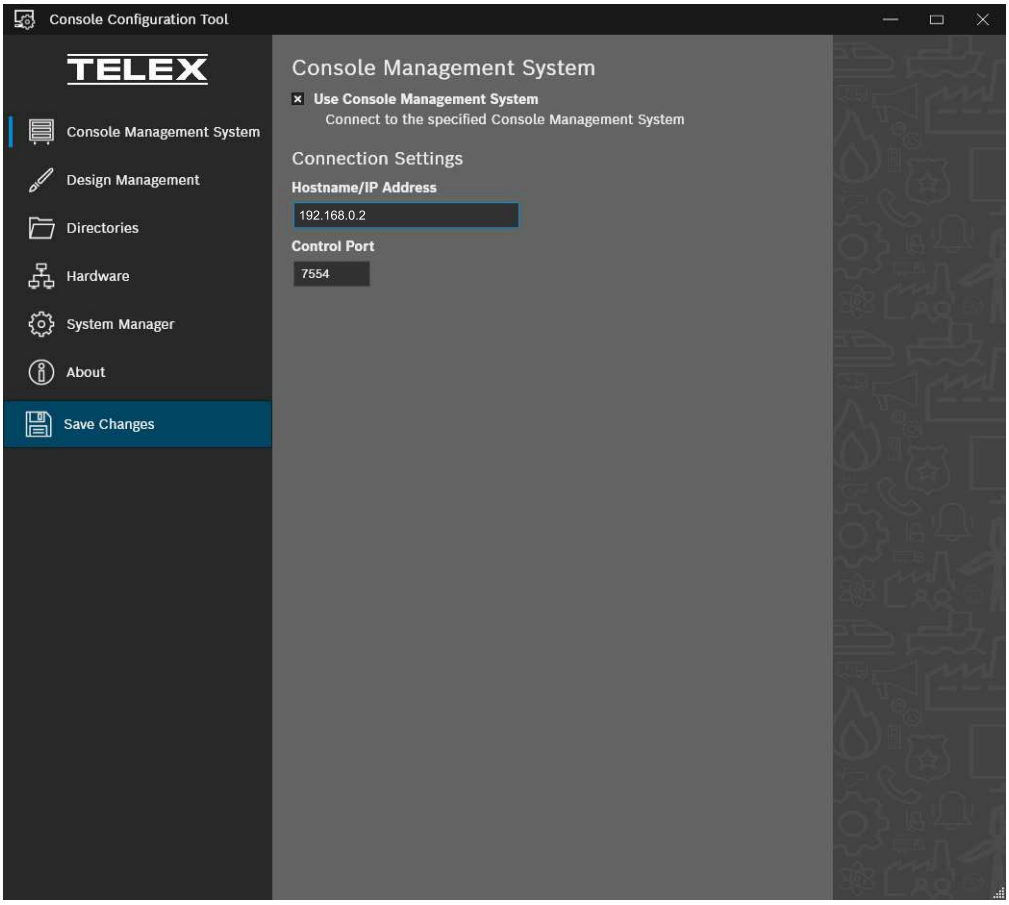
The **Backup Log in Mode** section defines what C-Soft does when there is no connection to CMS.

- Select the **Use last launched design radio button** to indicate the console should launch the last design used.
- Select the **Show list of local designs radio button** to indicate the console should display a list of recently-used local designs.

9.3.1 Configure Connection to CMS

To **configure a dispatch position for alias updates**, do the following:

1. Open the **Console Configuration Tool**.
2. Navigate to the **Console Management System page**.



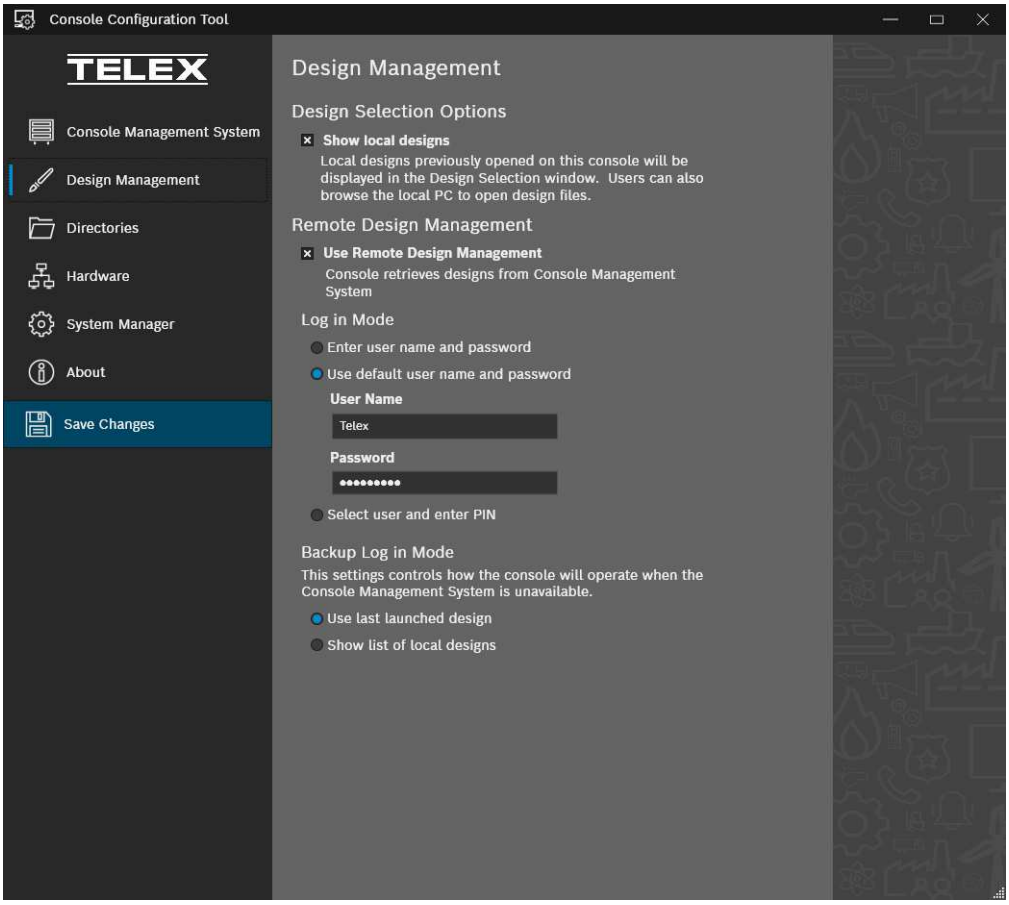
3. Select the **Use Console Management System check box**.
4. Enter the **Hostname or IP Address for CMS**.
5. Enter the **Control Port for CMS**.
6. Click **Save Changes**.

Notice!
If using CMS' Alias Management or CryptoSync features, these values have likely already been set. If configuring alias updates on an IP-30XX, we recommend using TSM.

9.4 Configure Design Manager

Use the Design Manager Page in the Console Configuration Tool to configure design C-Soft is to use. To configure the Design Manager do the following:

1. Open the **Console Configuration Tool**.
2. Navigate to the Design Management page.



3. Select the **Show local designs check box** to show a list of recently opened designs. You can then browse the list.
4. Select the **Use Remote Design Management check box** to have C-Soft try to log into CMS upon startup.
   If selected, the Log In Mode fields become active.
5. Select the **Enter user name and password radio button** to require the user to log in every time.
   OR
   Select the **Use default user name and password radio button** to use the default user name and password entered below.
6. If using the default user name and password:
   – Enter the **User Name**.
   – Enter the **Password**.
7. Select the **Use last launched design radio** button to use the last designed used.
   OR
   Select the **Show list of local designs radio button** to show a selectable list of local designs.
8. Click **Save Changes**.

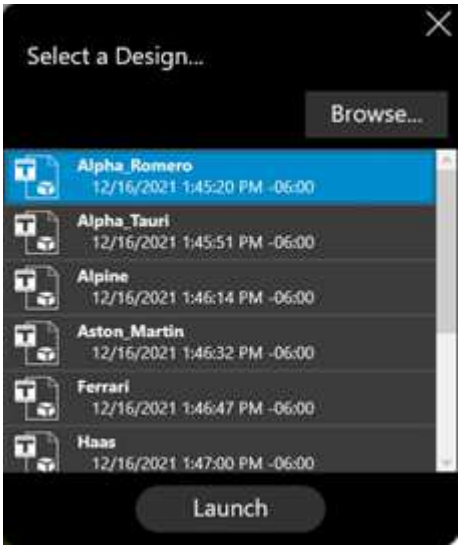
9.5 C-Soft Launch Operation

After CMS and C-Soft settings are fully configured for use with CMS's TDA File Manager, C-Soft's Design Management feature is ready to use.

1. Launch **C-Soft Runtime**.
   The Dispatch Login screen appears.

If default username and password is enabled, the default Username and Password are automatically applied and used to log in. Skip to Step 5.

1. Enter the **Username and Password** of a User configured in *Manage Users, page 20*.
2. Press the **Login button**.
   If only one design is assigned to the user (or user's role) in *CMS Design Repository, page 40*, C-Soft immediately launches to that design. If multiple designs are assigned to the user (or user's role), Console Launcher displays a list of designs available.
3. Select a design from the list.



4. Press the **Launch button**.

To **log in with a different user**, do the following:

1. Exit **the application**.
2. Re-launch **C-Soft Runtime**.

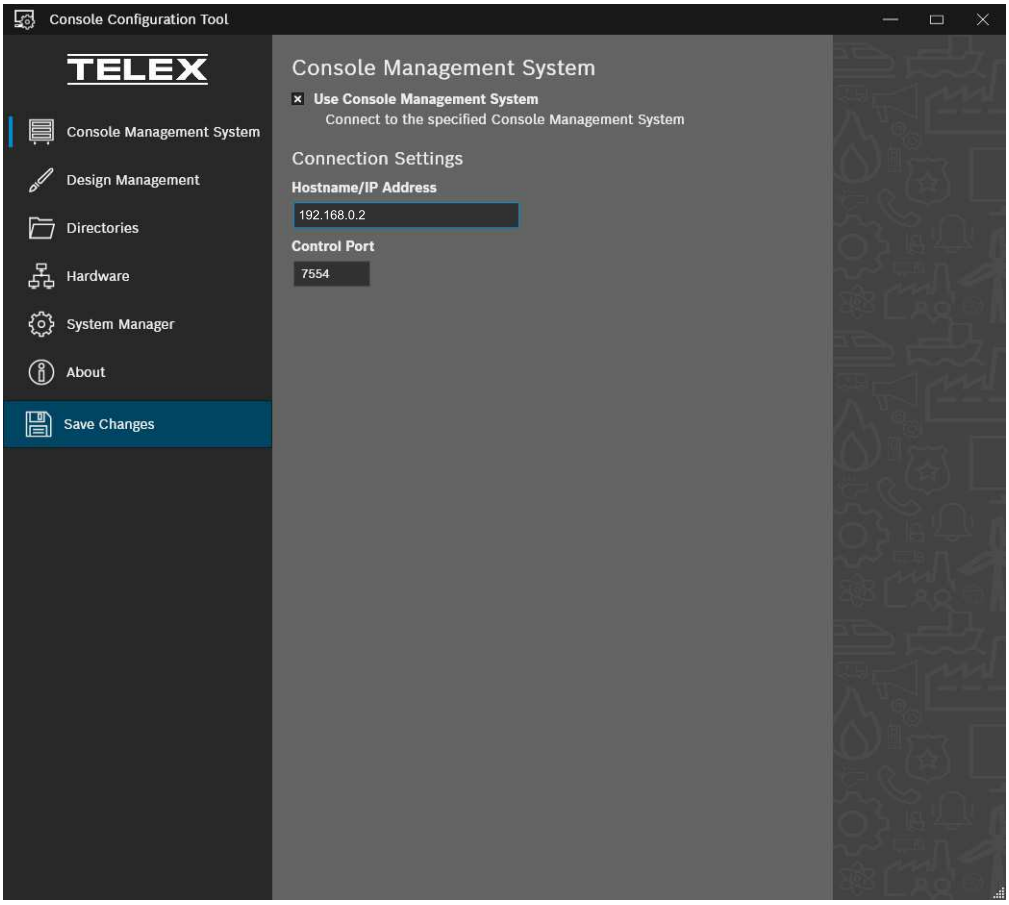
10 Contact Management and Operation

10.1 Dispatch Position Setup

10.1.1 Configure Connection to CMS

To **configure a dispatch position for alias updates**, do the following:

1. Open the **Console Configuration Tool**.
2. Navigate to the **Console Management System page**.



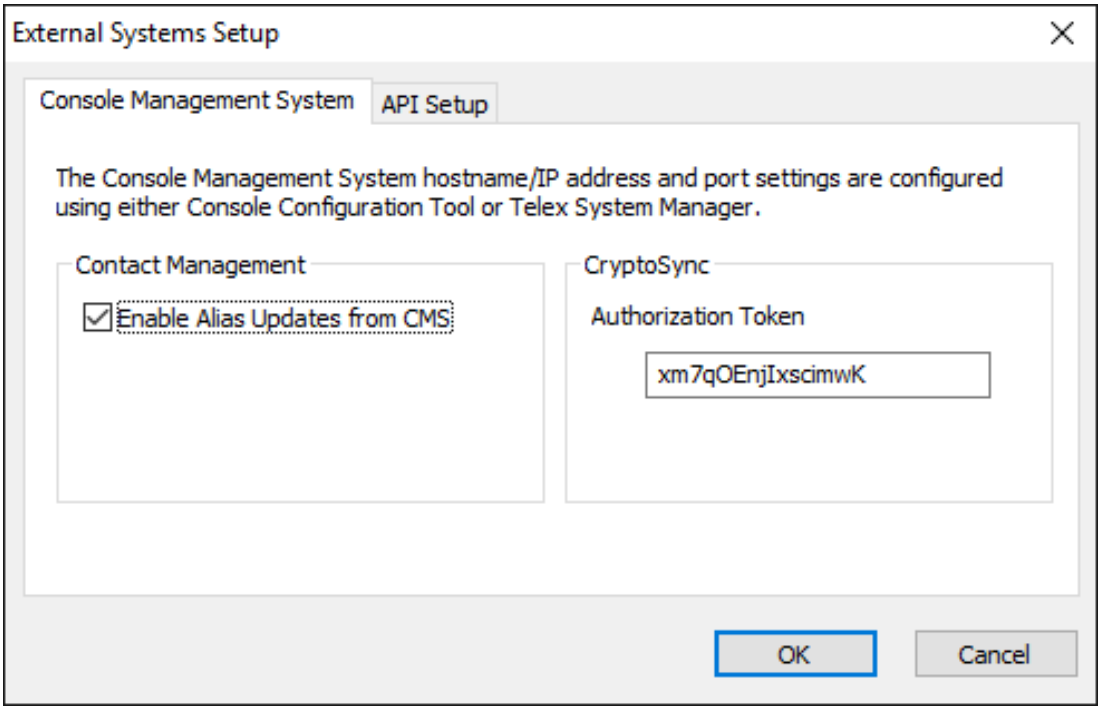
3. Select the **Use Console Management System check box**.
4. Enter the **Hostname or IP Address for CMS**.
5. Enter the **Control Port for CMS**.
6. Click **Save Changes**.

Notice!
If using CMS' Alias Management or CryptoSync features, these values have likely already been set. If configuring alias updates on an IP-30XX, we recommend using TSM.

10.1.2 CMS Alias Updates for the Design

To **configure C-Soft to retrieve alias updates from CMS**, do the following

1. Open **C-Soft Designer**.
2. From the Edit menu, select **External Systems Setup | Console Management System**.
   The External Systems Setup screen opens



3. Select the **Enable Alias Updates from CMS check box**.
4. Click **OK**.

10.2 Contact Manager Overview

The **CMS Manager Contact** menu contains the following items:

Users

The **User Contactstable** displays current user aliases. You can add new user aliases to this table. All Types are strict, as in for specific system types; the ID range must be valid for the system. Edit Aliases by selecting the edit icon on the respective alias' row.

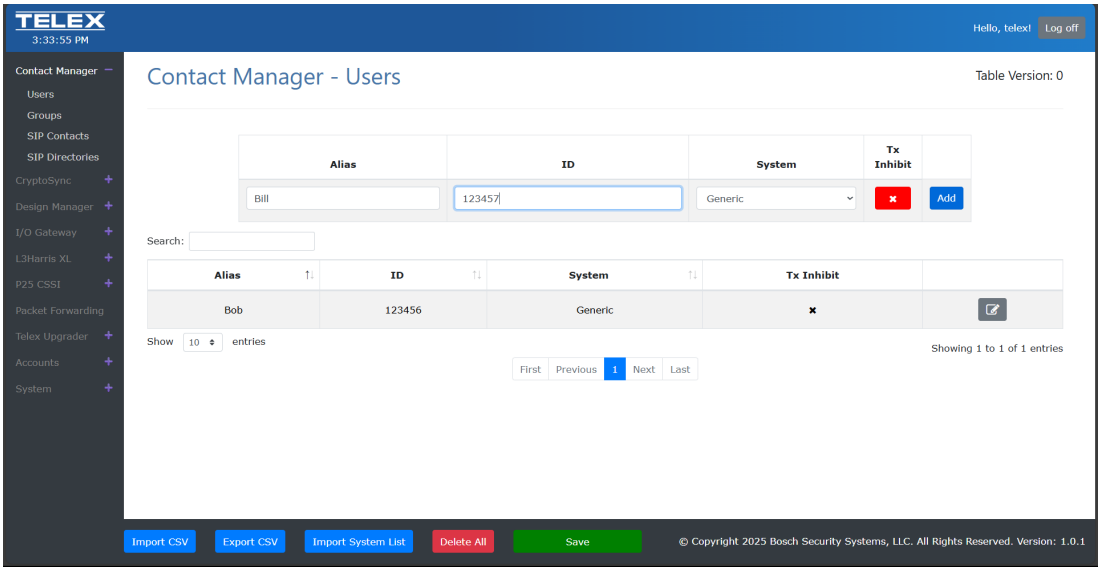


Figure 10.1: User Contacts

Groups

The **Contact Groups table** shows current group aliases. You can add new group aliases to this table. All Types are strict, as in for specific system types; the ID range must be valid for the system. Edit aliases by selecting the edit icon on the respective alias' row.

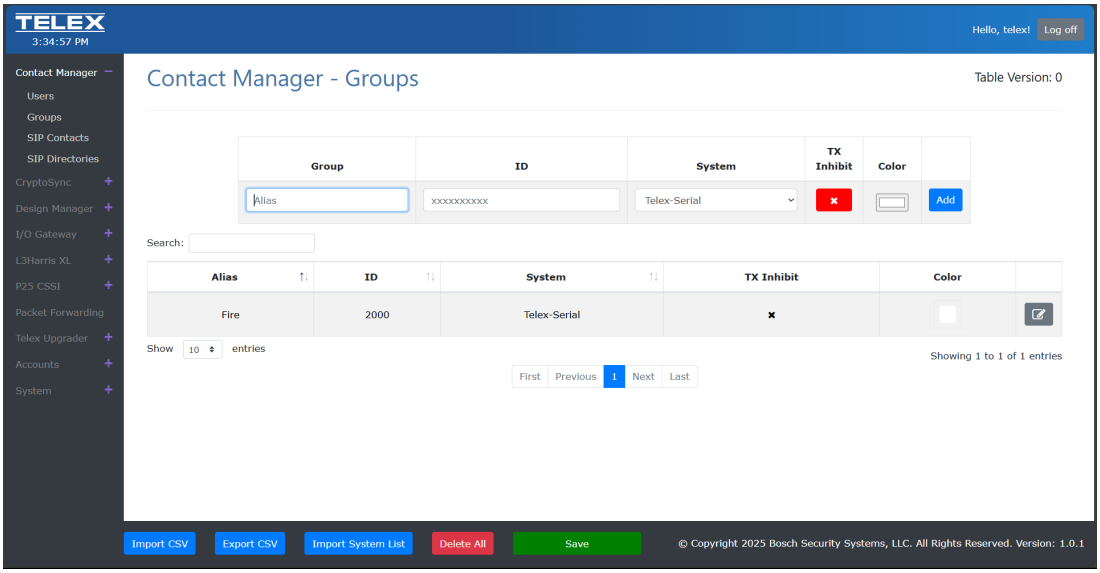


Figure 10.2: Contact Groups

SIP Contacts

The **SIP Contacts table** shows current SIP contacts. You can also add new SIP contacts to this table. Edit SIP contacts by selecting the edit icon on the respective row.

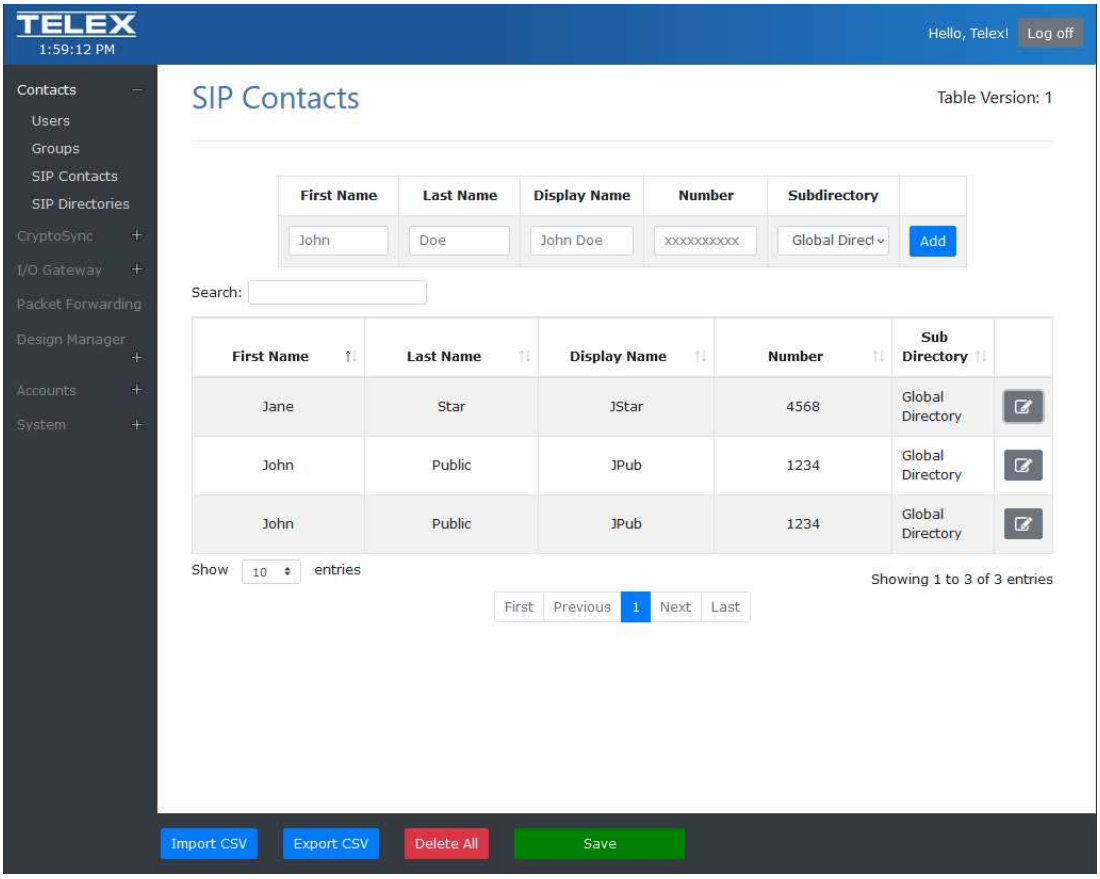


Figure 10.3: SIP Contacts

SIP Directories

The **SIP Directory table** shows current SIP directories in the system. You can add new SIP directories to this table. Edit SIP directories by selecting the edit icon on the respective row.

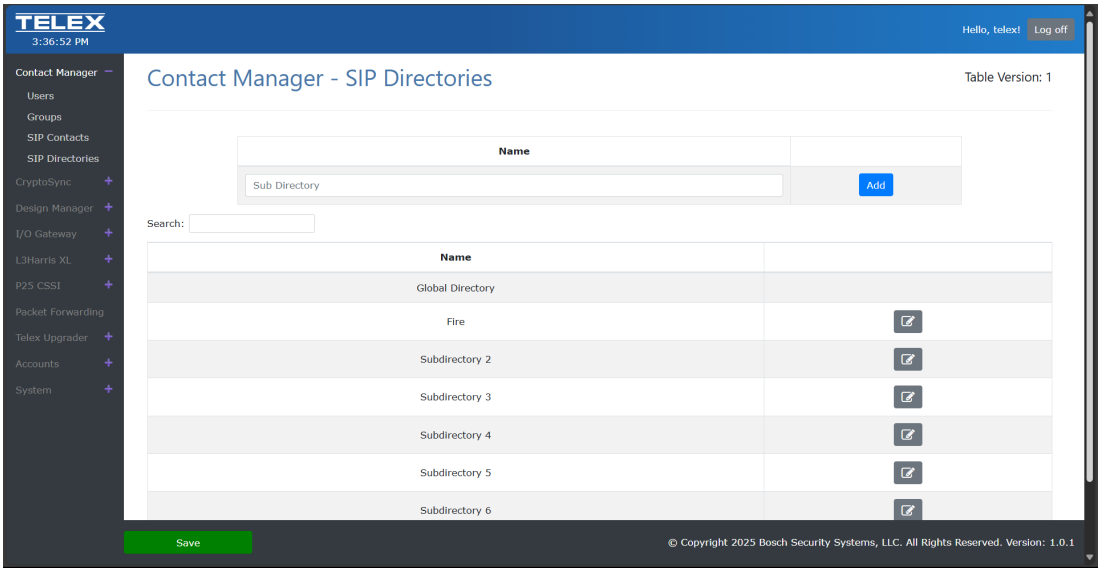


Figure 10.4: SIP Directories

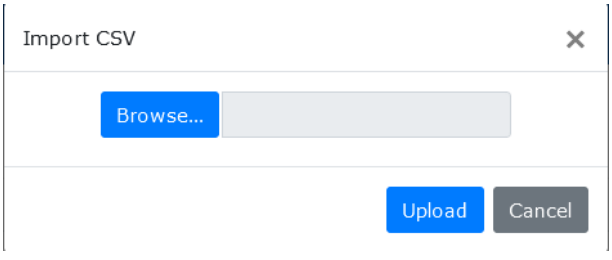
Notice!
In the lower left corner on each of these screens is a drop down box that lets you define the number of entries seen per page.

10.2.1 Search

The **Search** feature of the table allows a user to search for contacts with full or partial completeness of the alias or ID they are searching for.

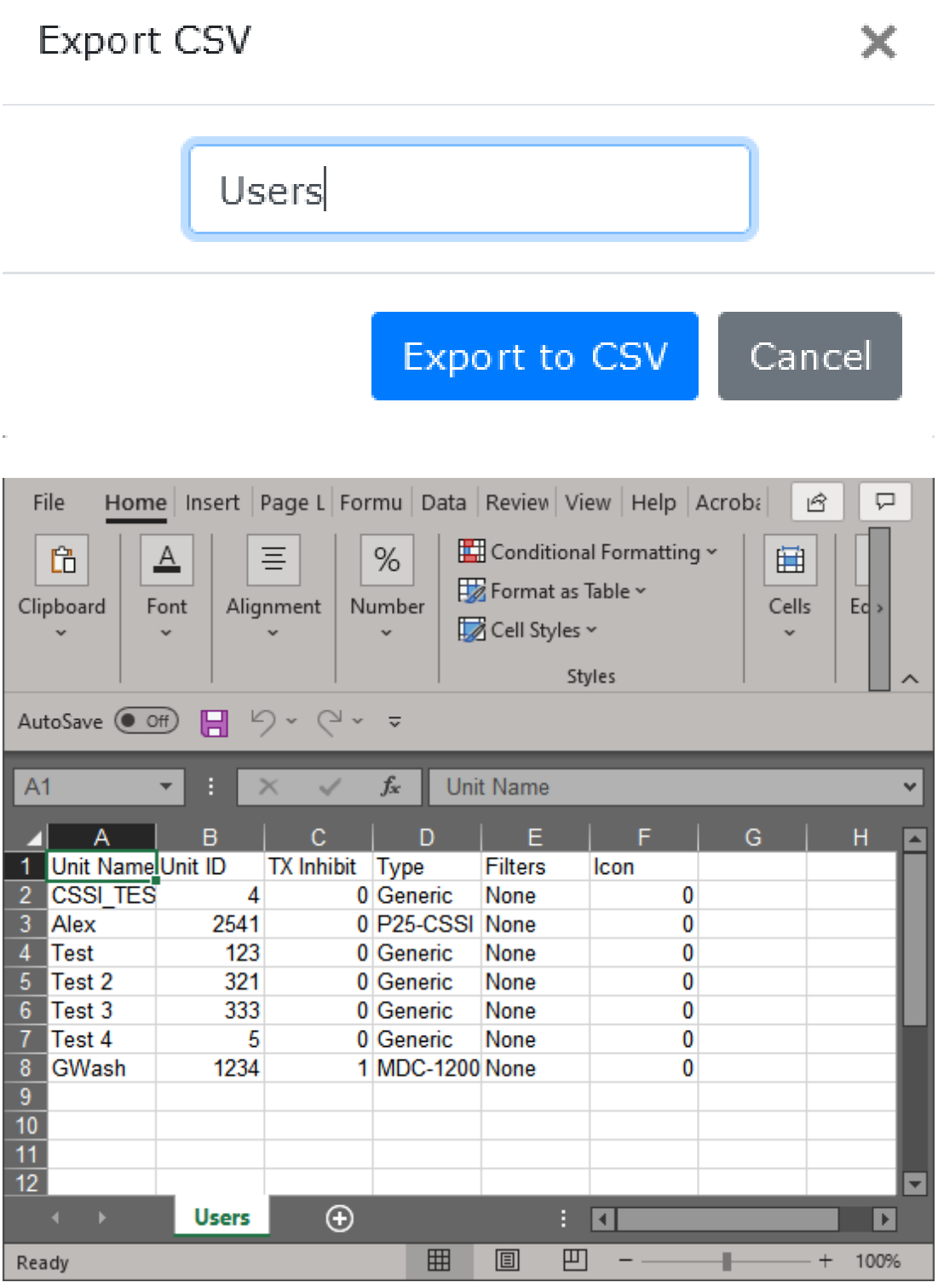
10.2.2 Import CSV

Import CSV allows the user to import user aliases from a CSV file exported from C-Soft Designer into the Contact Management module.



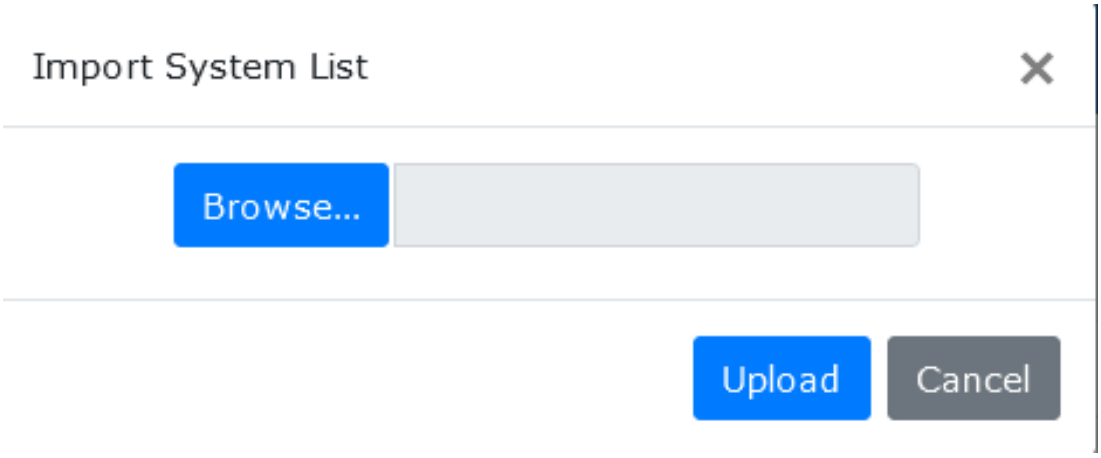
10.2.3 Export CSV

Export CSV allows the user to export user aliases to a CSV file.



10.2.4 Import System List

Import System List allows the user to import user aliases from a System List from an existing C-Soft design file into the Contact Management module.



10.2.5 Save

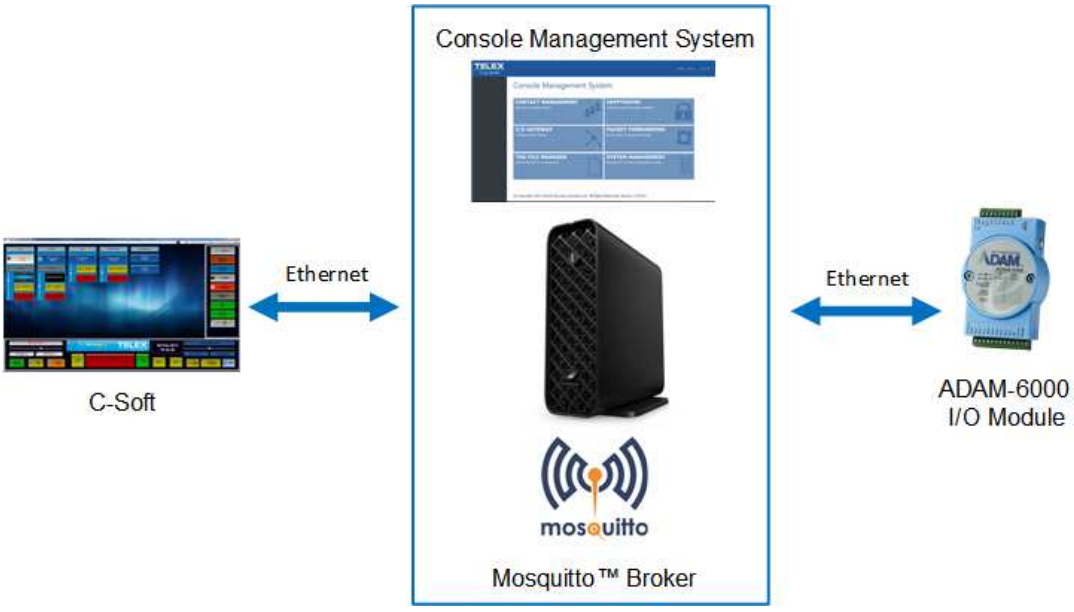
After adding, editing, deleting, or importing, the changes are not immediately saved to the systems database. Changes must be manually saved to the system.

11 I/O Gateway Configuration and Operation

Configuring the I/O Gateway requires the following components:

- Telex C-Soft console
- Telex Console Management System
- Eclipse Mosquitto™ MQTT Broker - this is pre-installed on the Telex Console Management System hardware.
- ADAM-6000 Series Ethernet I/O Module

System Connection



11.1 Broker Settings Page

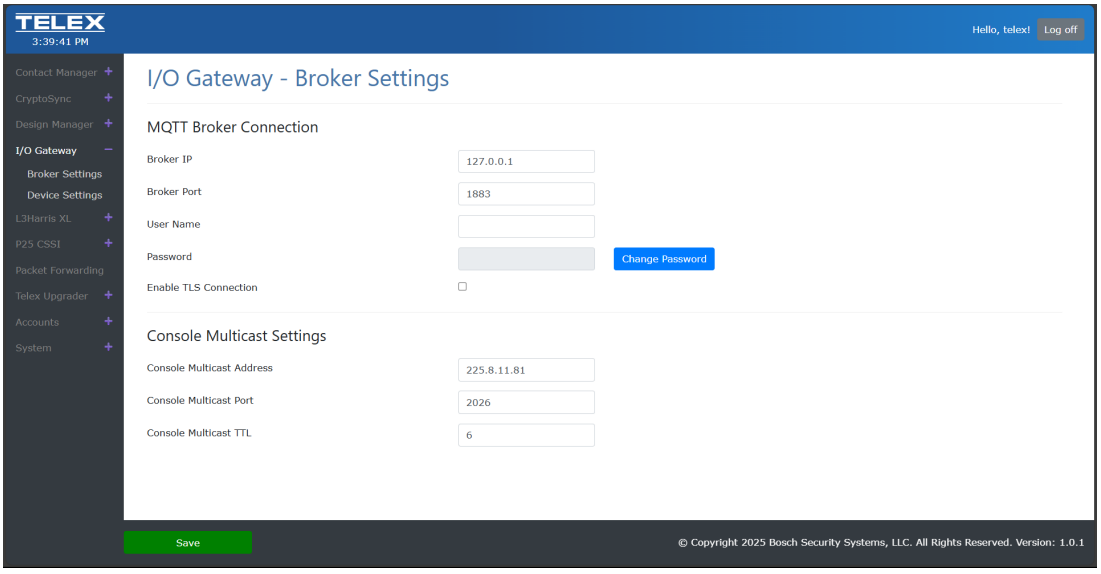


Figure 11.1: Broker Settings Page

MQTT Broker Connection

Broker IP Field

The **Broker IP** field defines the IP Address of the broker. If the Mosquitto broker running on the CMS PC is being used, use the Localhost address of 127.0.0.1.

Broker Port Field

The **Broker Port** field defines the port used by the broker. By default, most brokers use pot 1883, if not using TLS; and use port 8883, if using TLS

User Name Field

Use the **User Name** field to enter the user name used for authentication to connect to the broker.

Password Field and Change Password Button

The **Password** field displays the password used for authentication to connect to the broker. If there is no password or the password needs to be changed, click the **Change Password** button. The Change password screen opens for editing.

Enable TLS Connection Check Box

The **Enable TLS Connection** check box secures the connection with TLS. If the check box is clear, TLS is not active.

Console Multicast Settings

Console Multicast Address Field

The **Console Multicast Address** field defines the NEO-10 Multicast address of the C-Soft consoles. The entry in this field should correspond to the entry in the NEO-10 Multicast field in C-Soft Designer|Edit|Setup Global Parameters|Peripherals.

Console Multicast Port Field

The **Console Multicast Port** field defines the NEO-10 Update port of the C-Soft consoles. The entry in this field should correspond to the entry in the NEO-10 Update Port field in C-Soft Designer|Edit|Setup Global Parameters|Peripherals.

Console Multicast TTL Field

The **Console Multicast TTL** field defines the number of routers a multicast packet can go through before it stops.

The range for this field is 1 to 99.

11.2 Device Settings Page

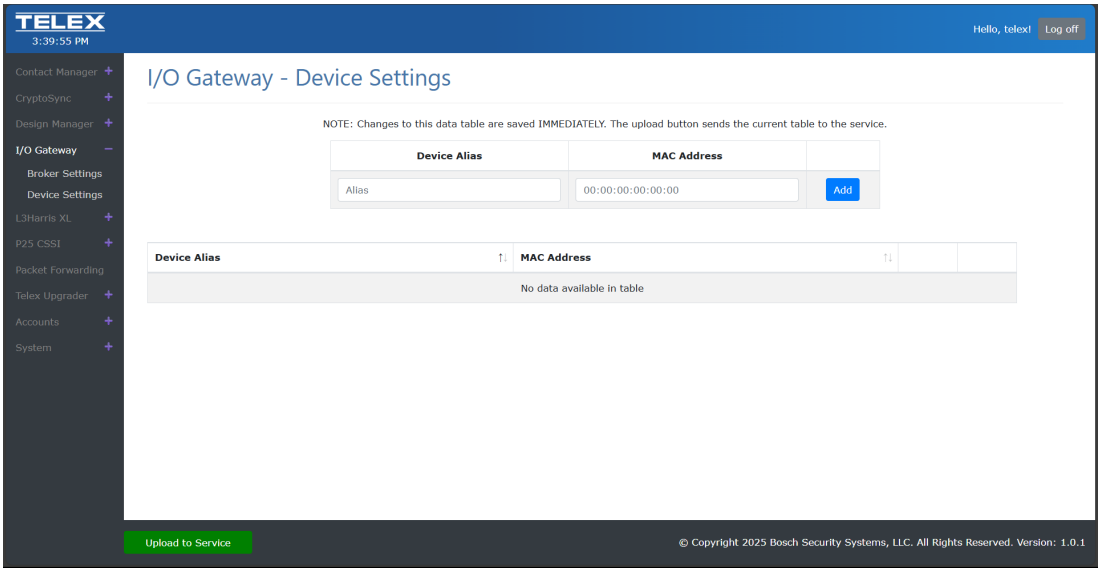


Figure 11.2: Device Settings Page

Alias Field

Use the **Alias** field to enter the name of the device being added.

MAC Address Field

Use the **MAC Address** field to enter the MAC address of the device being added.

Add Button

Use the **Add** button to add the device to the device list.

Device Alias Column

The **Device Alias** column displays a list of current devices in CMS.

MAC Address Column

The **MAC Address** column displays the MAC address for the device.

Edit Button

The **Edit** button opens the Edit screen. Modifications made and saved from this screen are immediately saved to the system.

Delete Button

The **Delete** button removes the device from the system.

11.3 ADAM-6000 Series Configuration

The ADAM-6000 comes with:

- 1 x ADAM-6000 Series Ethernet I/O Module
- 1 x ADAM-6000 Series Mounting Plate

11.3.1 Hardware Setup

To **set up an ADAM-6000 Series device**, do the following:

1. Connect a **DC power adapter to the unit**.
   The unit accepts any power supply that supplies input power within the range of +10 to 30 VDC. Screw terminals +VS and GND are for wiring the power supply.
2. Connect an **Ethernet cable** to the unit.
3. Attach **relay wires** to the desired relay screw terminals.

ADAM-6050	Terminal DO 0 and Iso GND are used for Relay #1, terminals DO 1 and Iso GND are used for Relay #2, etc.
ADAM-6060	Terminals RL 0+ and RL 0- are used for Relay #1, terminals RL 1+ and RL 1- are used for Relay #2, etc.
ADAM-6266	Terminals RL0 COM, RL0 NC, and RL0 NO are used for Relay #1, terminals RL1 COM, RL1 NC, and RL1 NO are used for Relay #2, etc.

4. Attach **input wires** to the desired input screw terminals and to Iso GND terminal.
   Terminal DI1 is used for Input #1, terminal DI2 is used for Input #2, etc.

11.4 TLS Operation

TLS (Transport Layer Security) encrypts data that is sent over the Internet. To ensure your data is secure, configure TLS on your system. Enabling TLS on your system requires you to configure the Mosquitto Broker, enable TLS in CMS, and enable TLS in the individual ADAM devices.

11.4.1 Configure the Mosquitto Broker

Notice!

This operation requires some experience in Linux. If done incorrectly the mosquitto broker may no longer work. We recommend that a Linux system administrator or a user with Linux system administration experience configure the mosquitto broker.

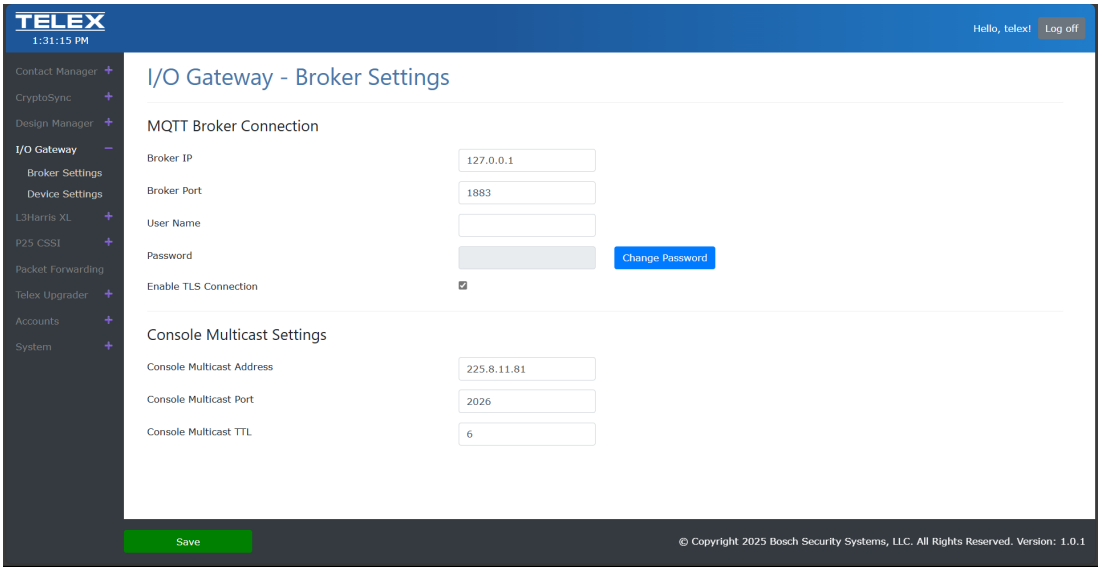
Notice!
This guide assumes you have not modified the default mosquitto conf file. If you have already modified the file, then replace any of the following steps to the modified file name.

To **configure the Mosquitto broker**, do the following:

1. **SSH** into the CMS unit with an SSH client as the telex user and the password set during configuration.
2. Using a terminal text editor, edit the following file with **sudo: /usr/lib/system/mosquitto.service**. Use the root password set in configuration.
3. Under [Service], modify the following line:
   from: ExecStart=/usr/sbin/mosquitto -c /etc/mosquitto/mosquitto.conf
   to: **ExecStart=/usr/sbin/mosquitto -c /etc/mosquitto/mosquitto_tls.conf**.
4. Save the **file**.
5. Run the command: **sudo systemctl restart mosquitto.service**.
   Mosquitto is now configured to use tls/ssl.

11.4.2 Enable TLS in CMS

1. Navigate to **I/O Gateway | Broker Settings** page.
   The Broker Settings page opens.



2. Set the Broker Port to **8883**.
3. Select the **Enable TLS Connection checkbox**.
4. Click the **Save button**.

11.5 User Name and Password Operation

Username and Password operation is used to authenticate individual devices in the system. When enabled, only allowed devices can connect to the broker. Enabling User Name and Password operation on your system requires you to configure the Mosquitto Broker, add a broker-connection username and password to CMS, and to add a user name and password in the ADAM devices. Username and Password operation also requires that TLS be enabled both in CMS and in the ADAM devices.

11.5.1 Mosquito Broker Configuration

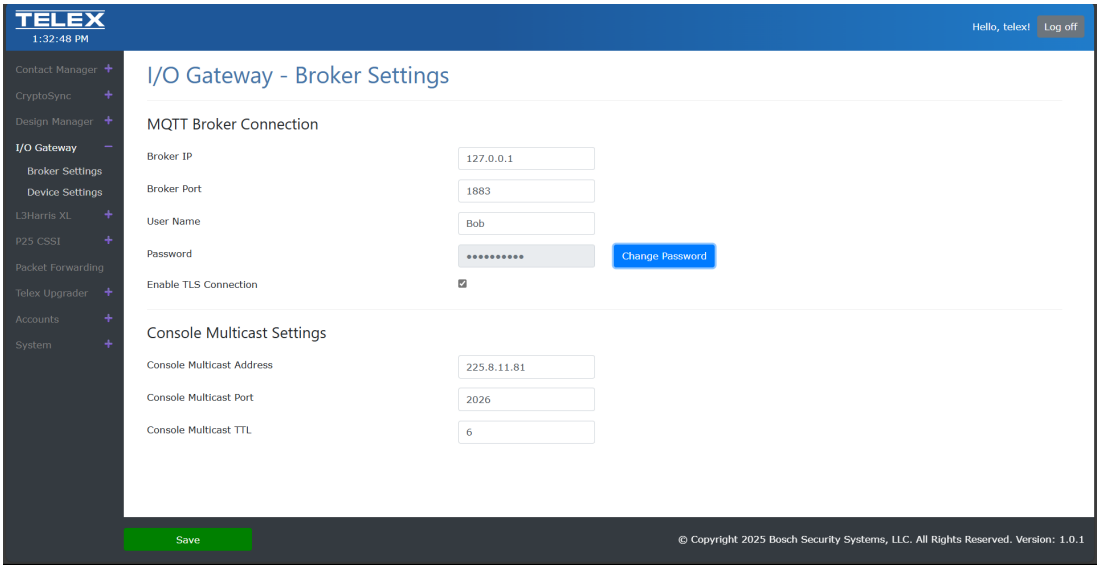
Notice!
This operation requires some experience in Linux. If done incorrectly the mosquitto broker may no longer work. We recommend that a Linux system administrator or a user with Linux system administration experience configure the mosquitto broker.

Notice!
This guide assumes you have not modified the default mosquitto conf file. If you have already modified the file, then replace any of the following steps to the modified file name.

1. **SSH** into the CMS unit with an SSH client as the telex user and the password set during configuration.
2. Create a file in /etc/mosquitto/ called **password** with sudo.
3. Using a terminal text editor, edit the **password file** you just created with sudo.
4. Add users with the following syntax **user:password** on separate lines.
   User is the name of the user and password is the user's password.
5. Save and close the **file**.
6. Run the command: **sudo mosquitto_passwd -U /etc/mosquitto/password**.
7. Using a terminal text editor, edit the following **file** with sudo: **/usr/lib/systemd/system/mosquitto.service**.
   Use the root password set in configuration.
8. Under [Service] modify the following **line**:
   from: ExecStart=/usr/local/sbin/mosquitto -c /etc/mosquitto/**mosquitto.conf**
   to: ExecStart=/usr/local/sbin/mosquitto -c /etc/mosquitto/**mosquitto_tls_password.conf**
9. Save the **file**.
10. Run the command: **sudo systemctl daemon-reload**.
11. Run the command: **sudo systemctl restart mosquitto.service.**
    Mosquitto is now configured to use tls/ssl and user authentication

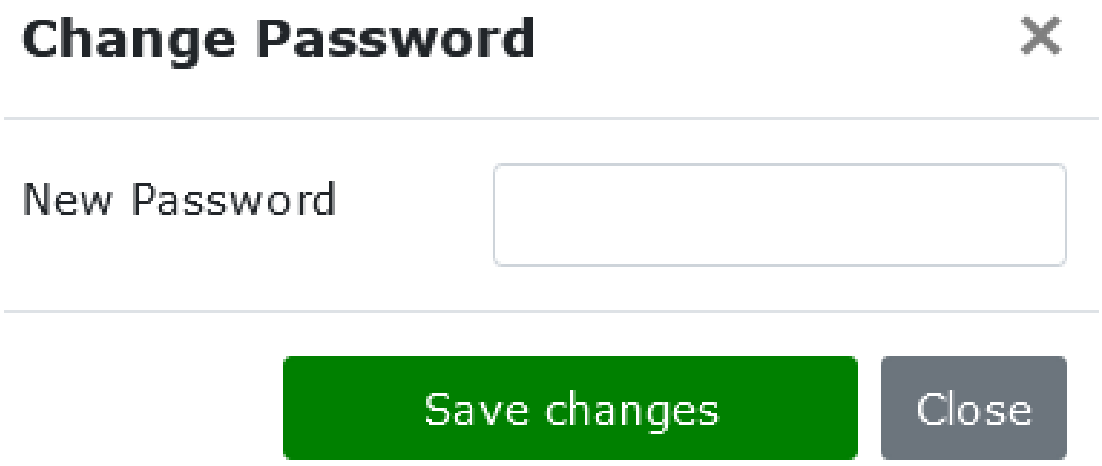
11.5.2 Console Management System Configuration

1. Navigate to the I/O Gateway Broker Settings page.



2. Enter a **user name**.

3. Click the **Change Password button**.
   The Change Password screen appears.

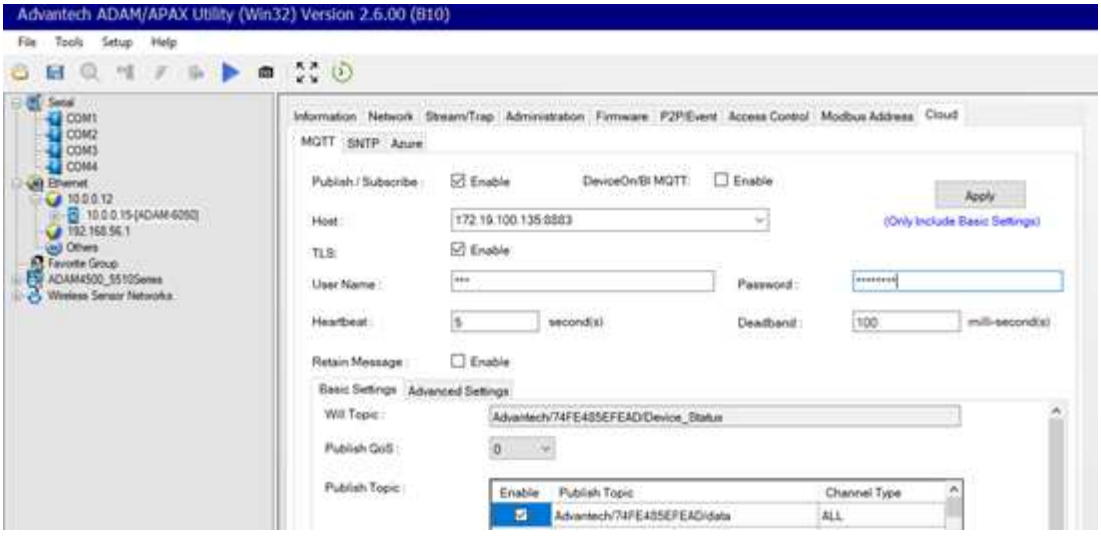


4. Enter a **password** in the New Password field.
5. Enable TLS, if not already enabled.
6. Click the **Save button**.

11.5.3 ADAM-6000 Series Configuration

To **configure an ADAM-6000 Series with a username and password**, do the following:

1. Open the **Advantech ADAM/APAX utility**.

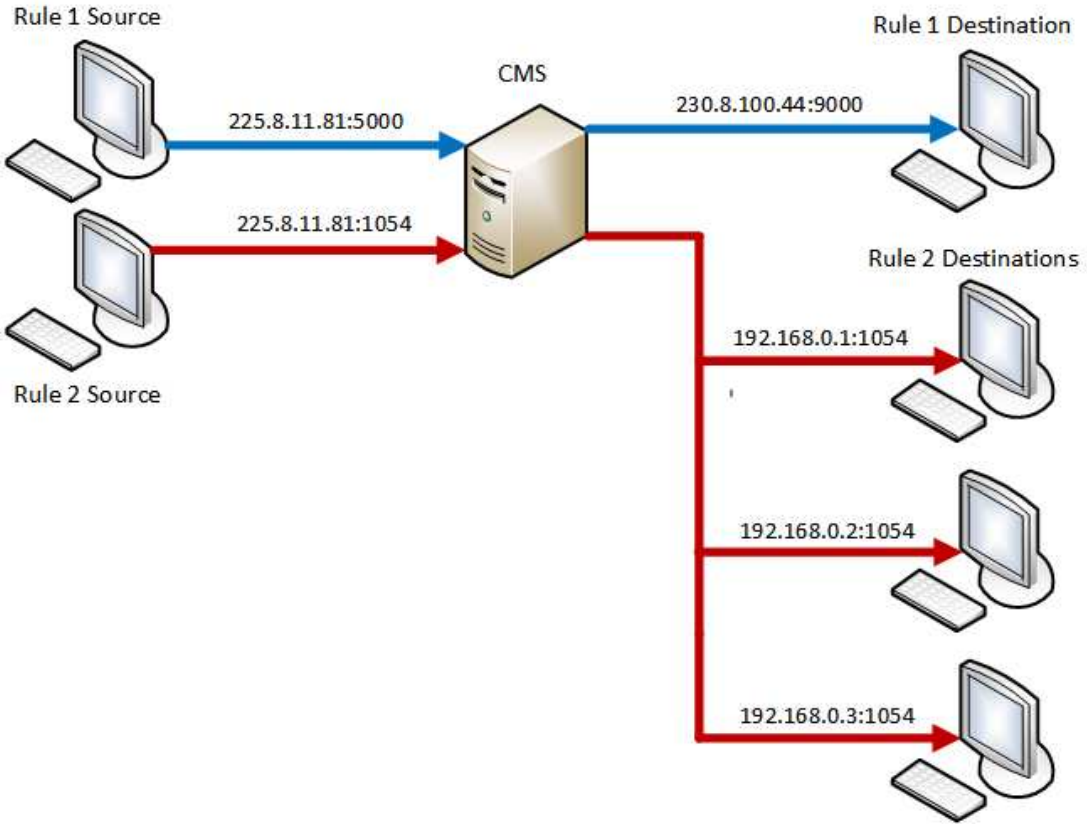


2. In the left navigation, find and select the **ADAM-6000 series unit**.
3. Select the **TLS Enabled checkbox**.
4. Click the **Cloud tab**.
5. Enter the **Username**.
6. Enter the **Password**.
7. Click the **Apply button**.

Notice!
It is recommended to restart the ADAM device after changing the username and/or password. This is done through the Administration tab on the Advantech ADAM/APAX utility.

12 Packet Forwarding Configuration and Operation

The Packet Forwarding module receives UDP packets on one address and port and then rebroadcasts the UDP packets on one or more different multicast/unicast addresses. The rebroadcast logic is contained in a mapping referred to as a Rule. A Rule is composed of a Source, which is the inbound packet address and port, and one or more Destinations, which are the outbound ports and addresses. Sources and Destinations support either unicast or multicast addresses. The diagram below shows the mapping of sources and destinations for two rules: Rule 1 and Rule 2.

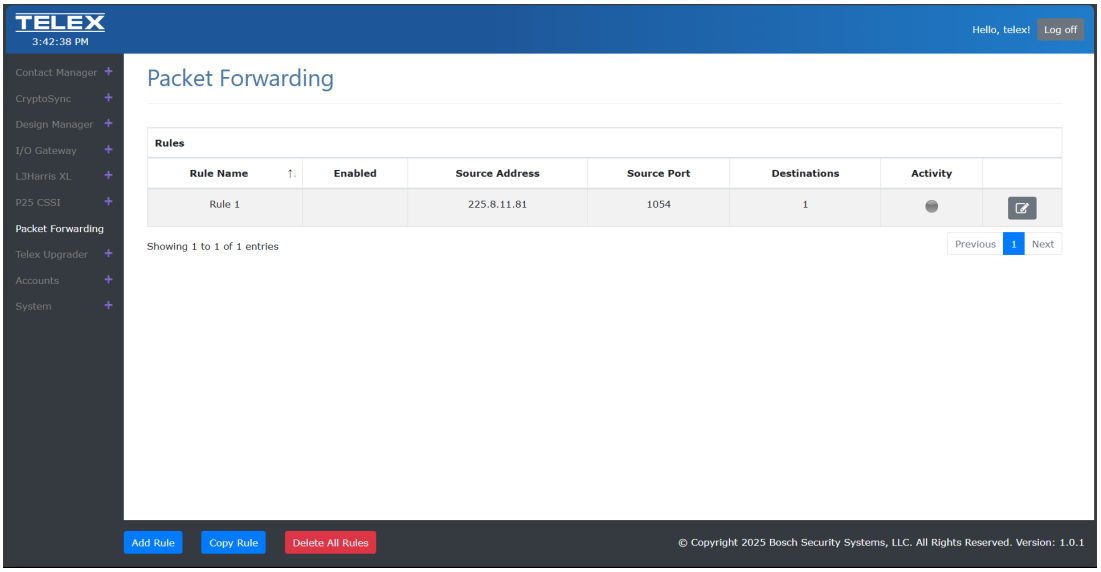


12.1 Edit Rule

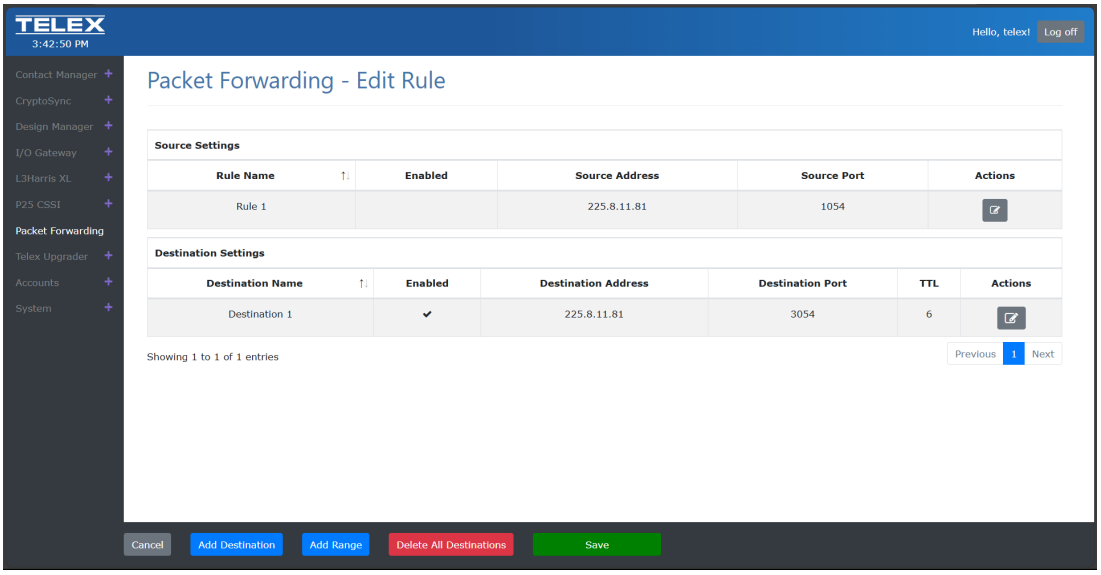
By default, the Packet Forwarding screen contains a single default Rule.

To **edit a rule**, do the following:

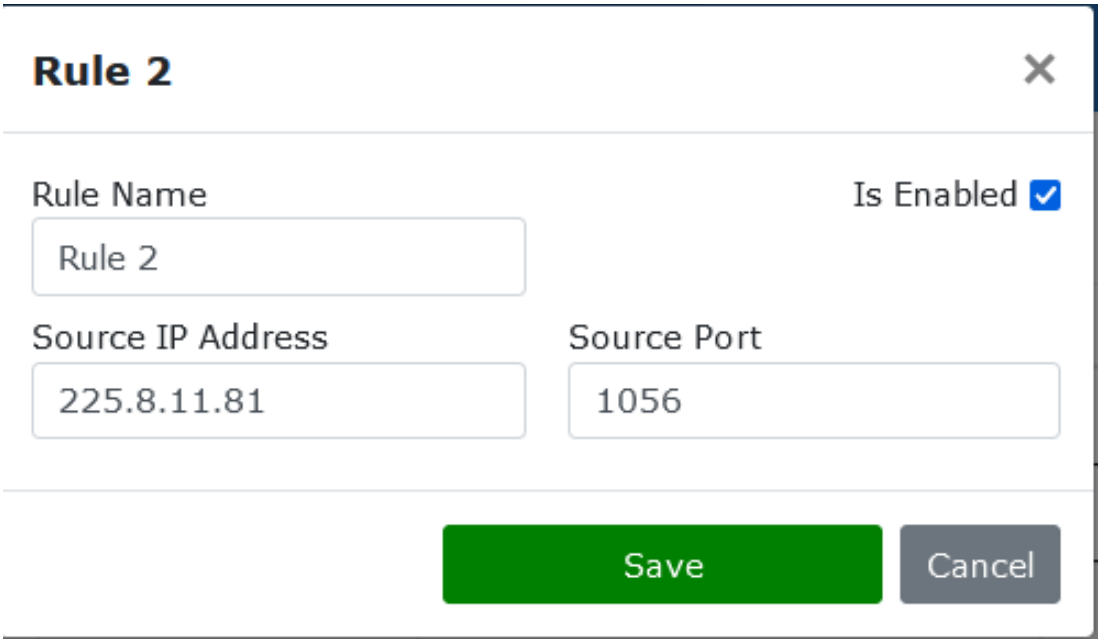
1. Navigate to the **Packet Forwarding page** on the Console Management Server.



2. Click on the **Rule's edit button**.
   The Edit Rule page opens.



3. Click the **edit icon next to the rule you want to modify**.
   The Source Setting screen opens.

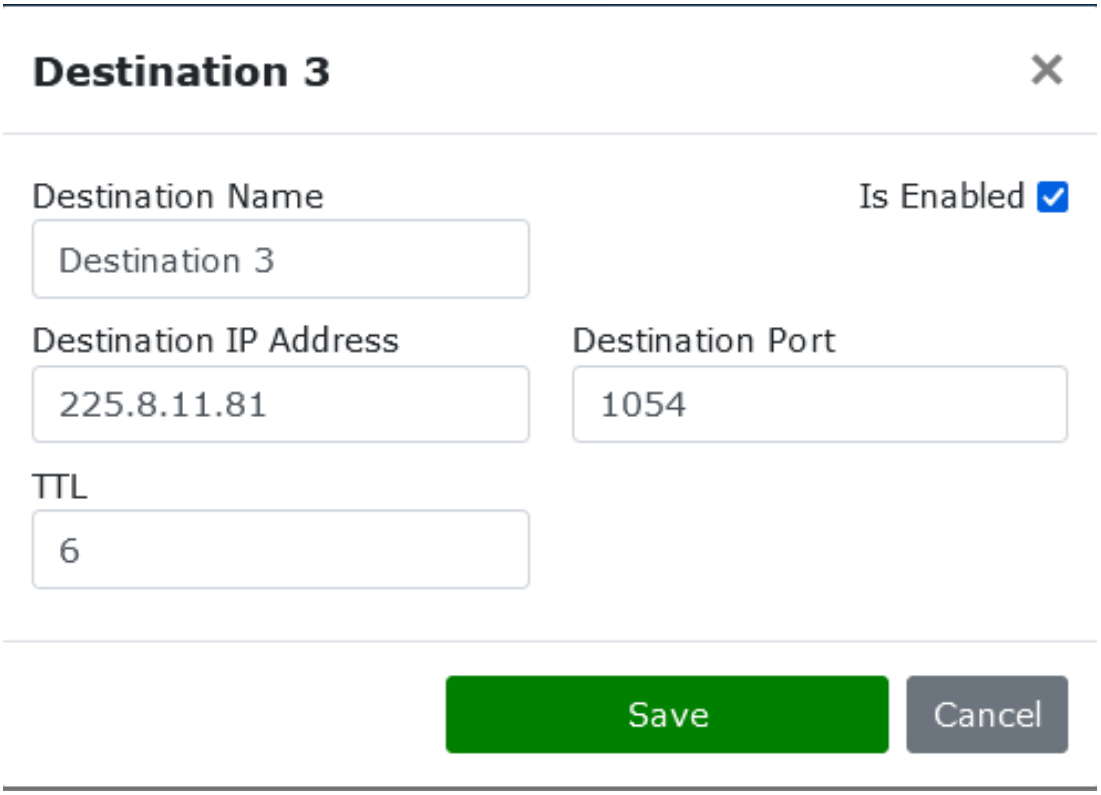


4. Make the **desired changes**.
5. Click the **Save button**.
   The Source Setting screen closes.

Notice!
The default rule is disabled by default. Select the Is Enabled checkbox to enable the Rule and allow UDP packets to rebroadcast.

To **edit the Destination settings**, do the following:

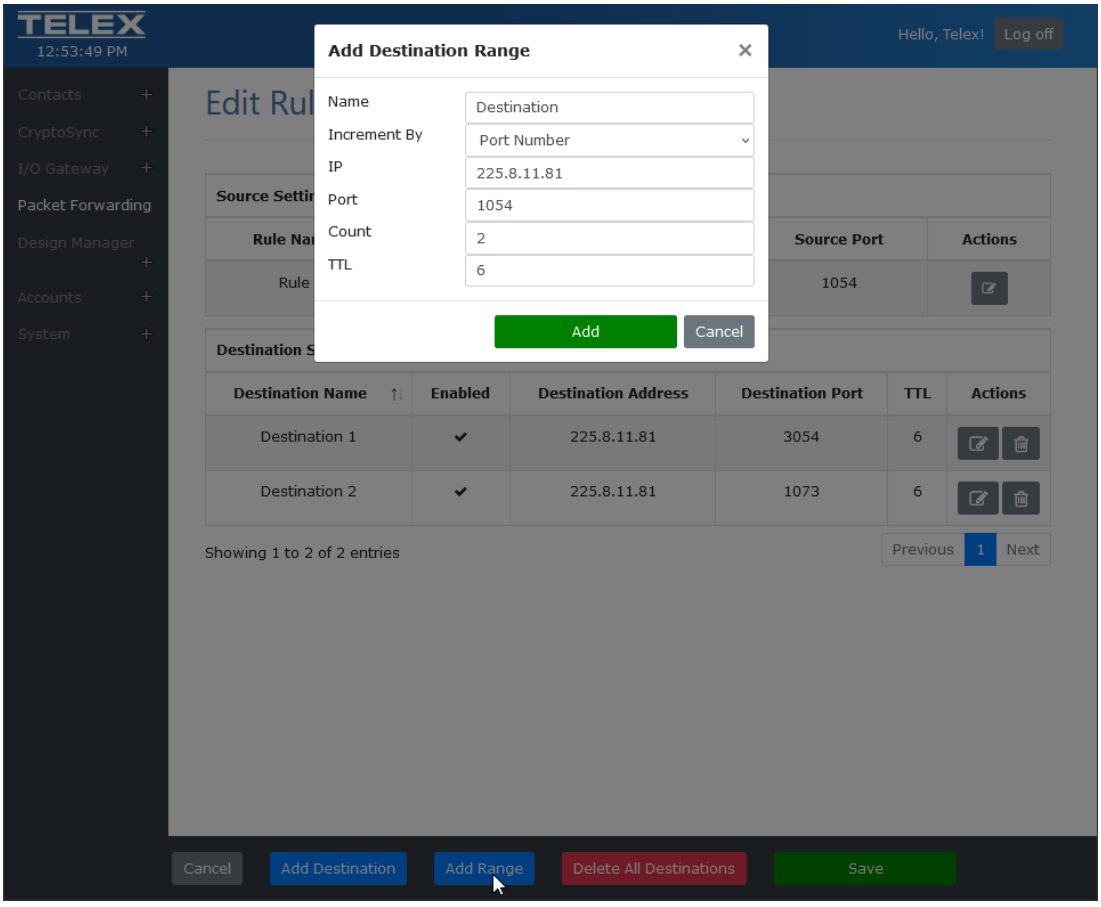
1. Click the **Destination Setting's edit button**.
   The Destination Setting screen appears.



2. Make the **desired changes**.
3. Click the **Save button**.

To **add a destination**, do the following:

1. Click the **Add Destination button** to add a destination to the rule.
2. Click the **Add Range button** to add multiple destinations on one time
   The Add Destination Range screen opens. A range of destinations can be incremented by either port number (i.e. 1054, 1055, 1056, etc) or by IP address (i.e. 225.8.11.81, 225.8.11.82, 225.8.11.83, etc). The Count field is the total number of new Destinations to be added.

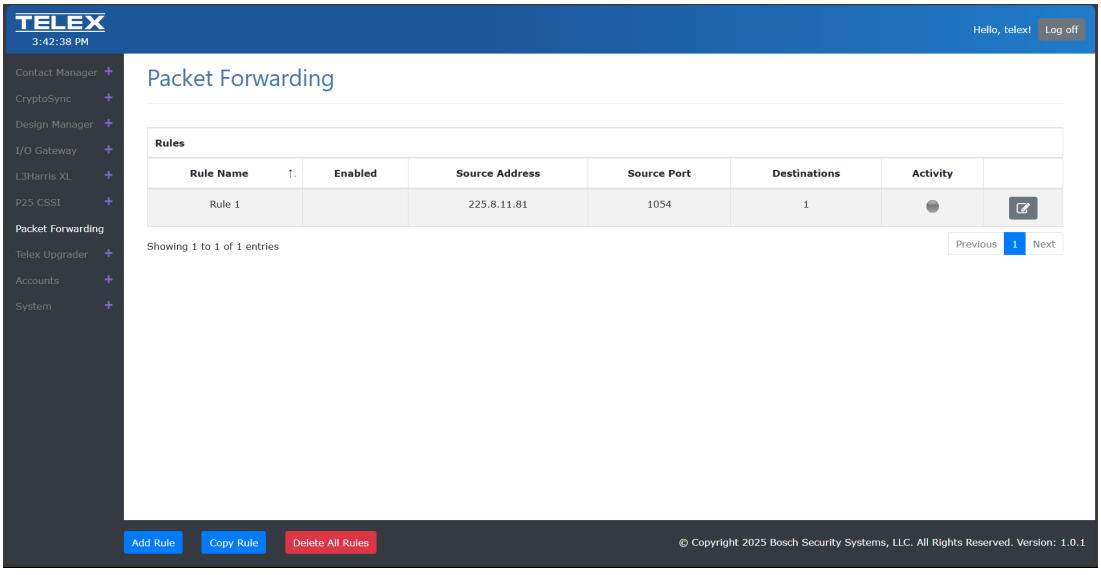


3. Click the **Add button**.
4. Click the **Save button**.

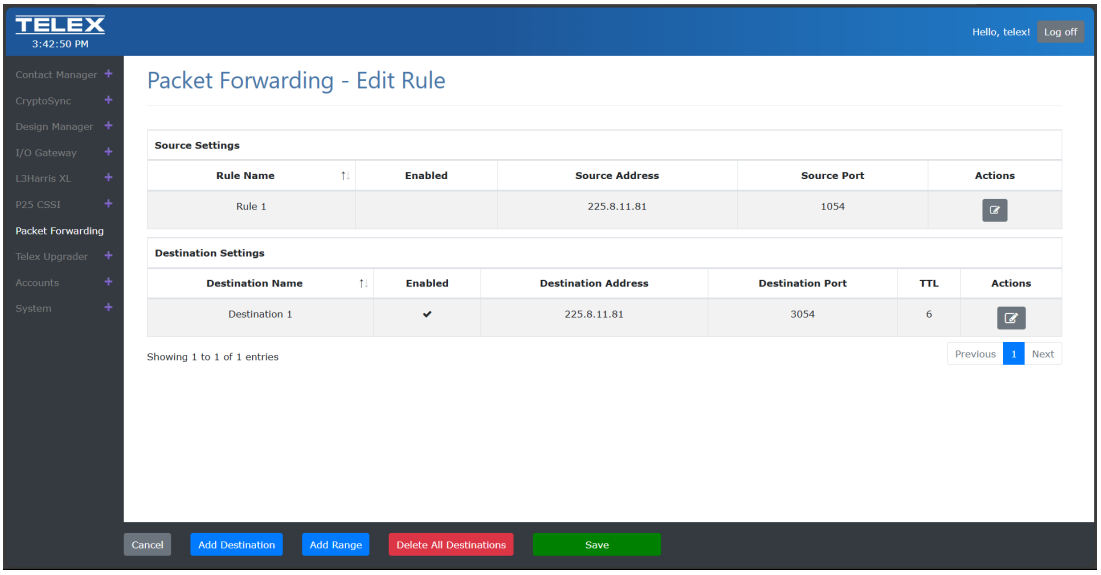
12.2 Add Rule

To **add a new rule to the rule list**, do the following:

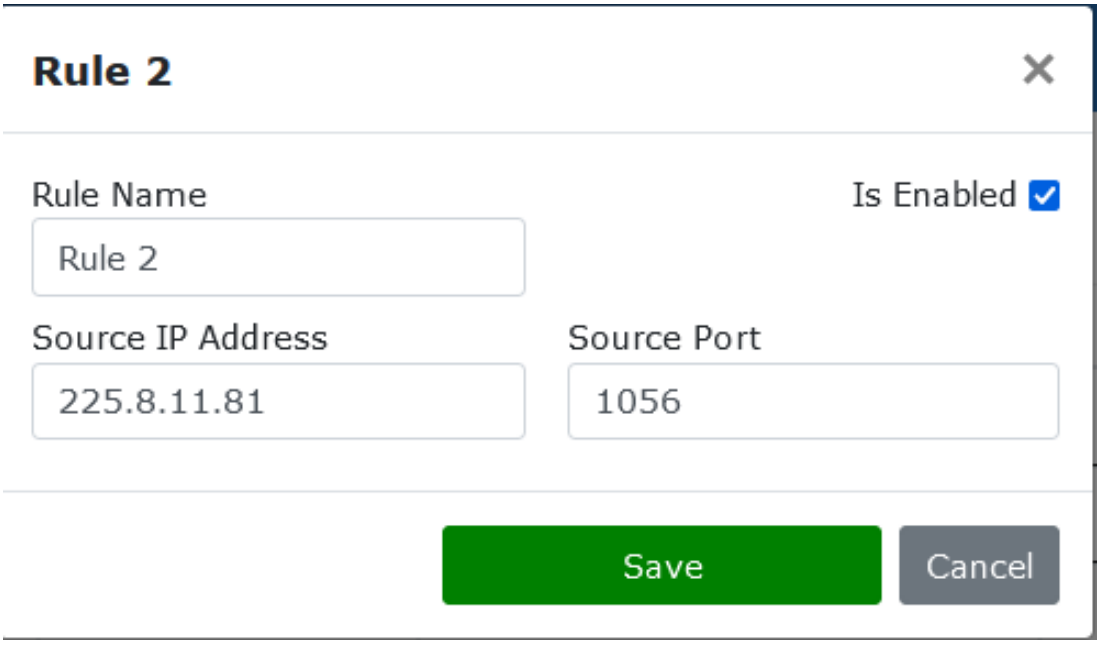
1. Navigate to the **Packet Forwarding page** on the Console Management Server.



2. Click the **Add Rule button**.
   The Edit Rule page opens.



3. Click the **edit icon next to the rule you want to modify**.
   The Source Setting screen opens.



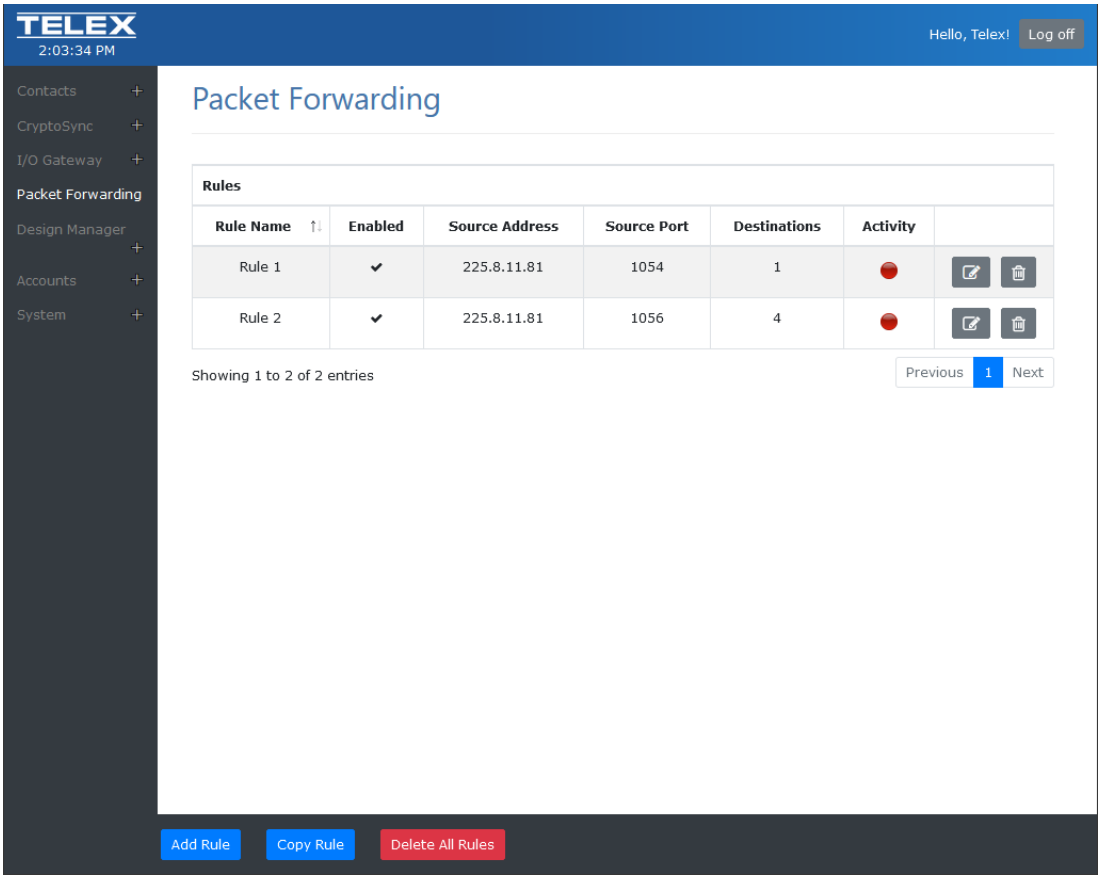
4. Make the **desired changes**.
5. Click the **Save button**.
   The Source Setting screen closes.
6. Click the **Save button**.

The new rule appears in the Rules list.

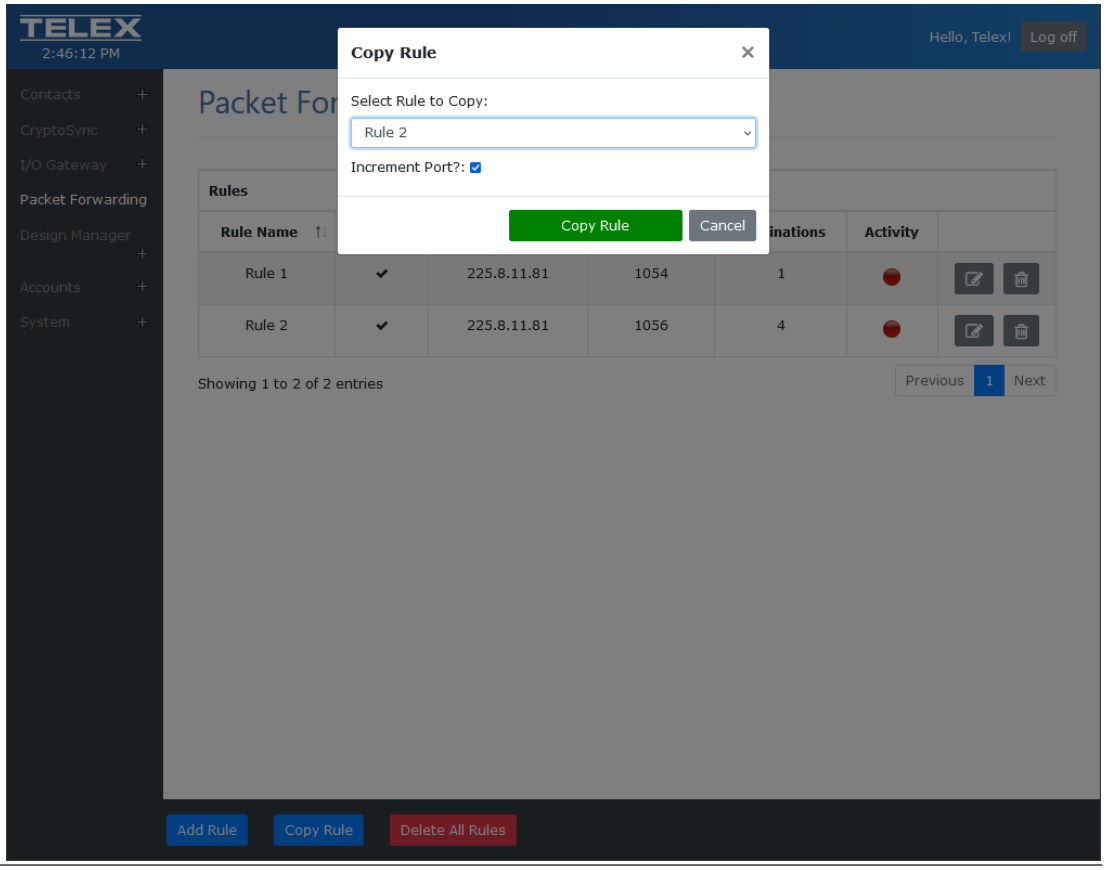
12.3 Copy Rule

To **create a rule from an existing rule**, do the following:

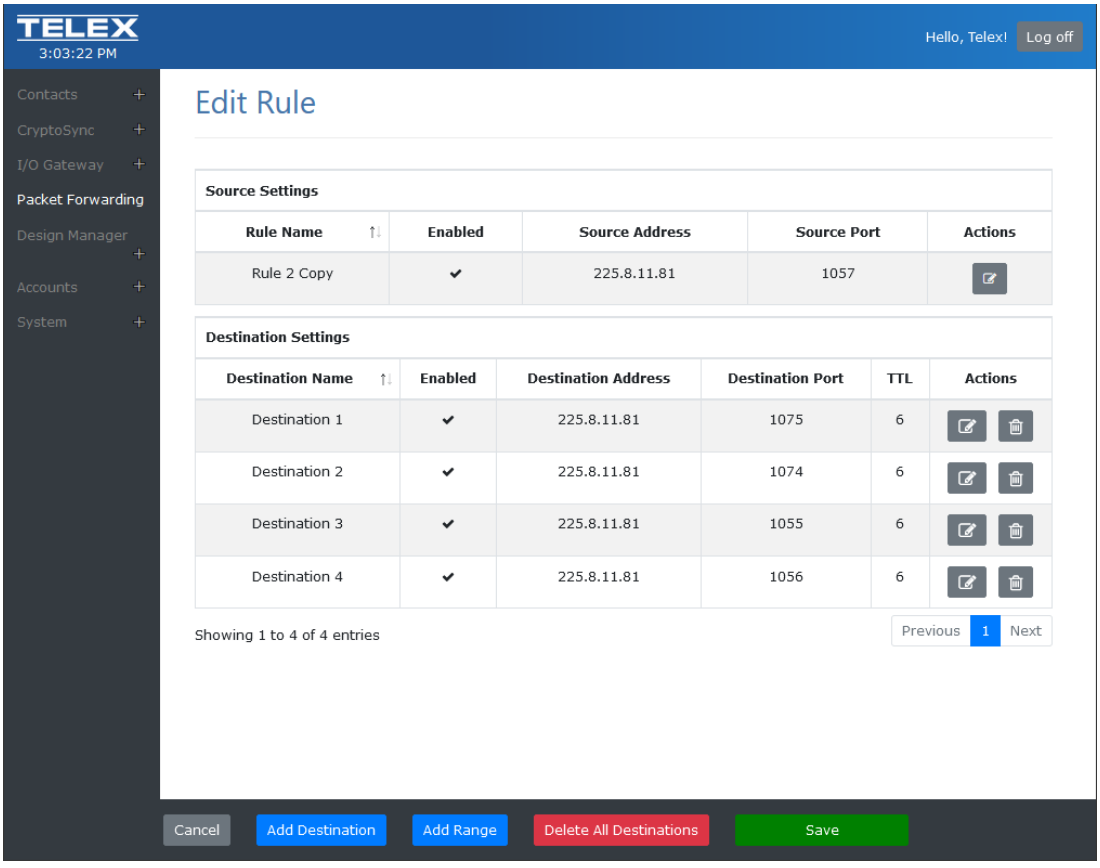
1. Navigate to the **Packet Forwarding page** on the Console Management Server.



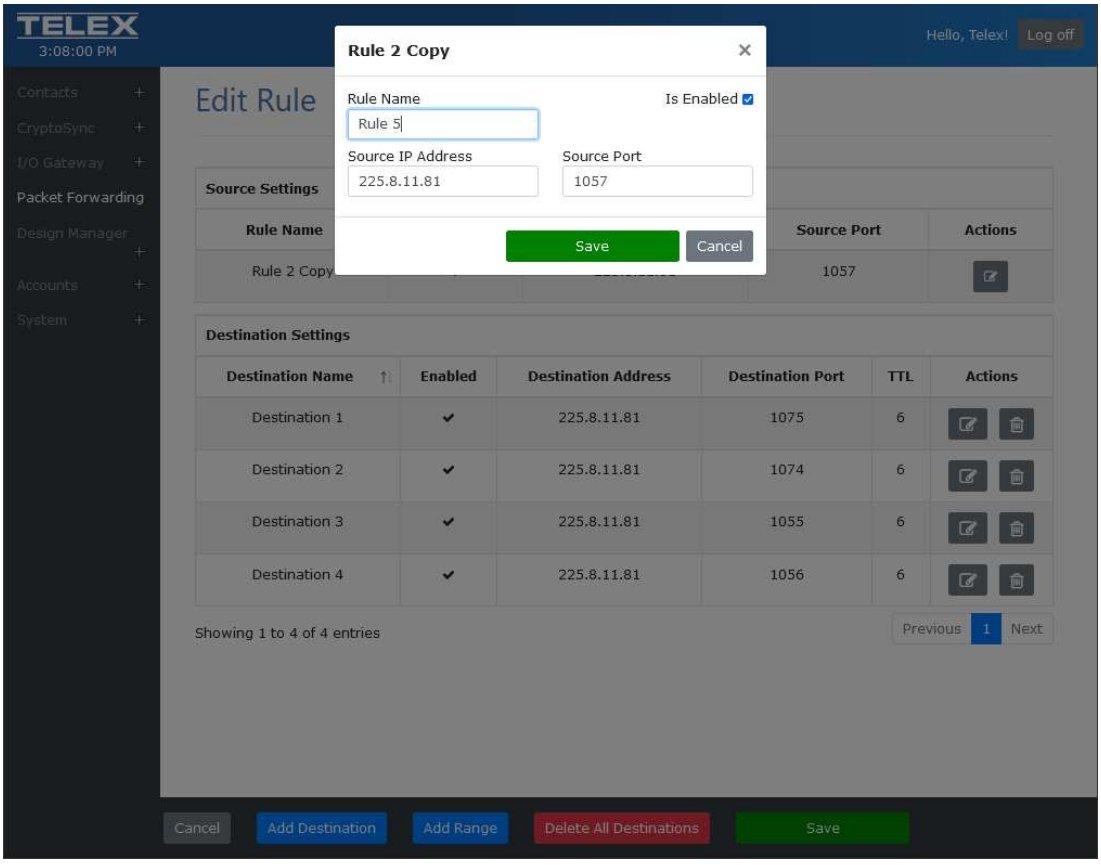
2. Click the **Copy Rule button**.
   The Copy Rule screen opens.



3. Select the **rule** to copy.
4. Select the **Increment Port? check box**, if desired.
5. Click the **Copy Rule button**.
   The Copy Rule page closes and the Edit Rule page appears.



6. Click the **Edit icon** next to copied rule.
   The Rule screen opens for editing.

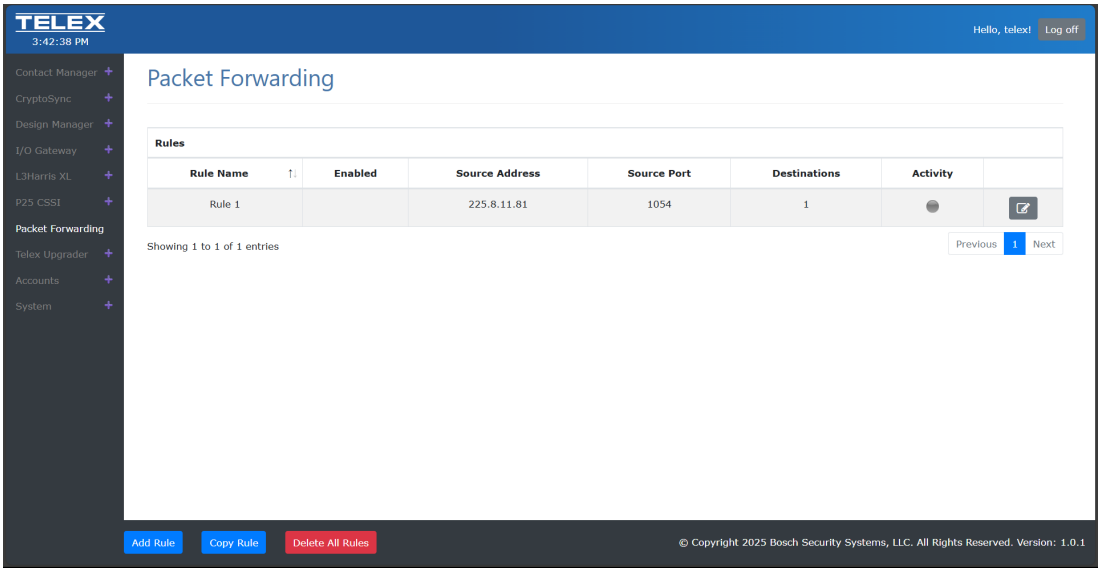


7. Change the **name** of the rule.
8. Click **Save**.
   The Rule Copy screen closes.
9. Click **Save**.
   The Packet Forwarding screen opens with the new rule in the list.

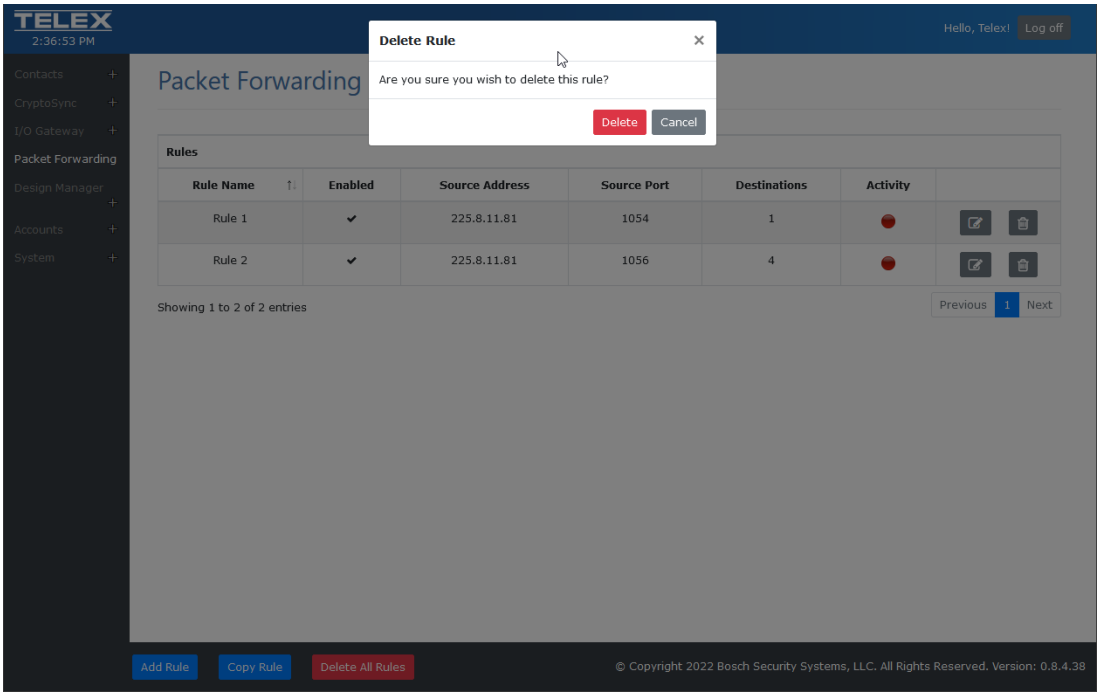
12.4 Delete Rule

To **delete a rule from the rule list**, do the following:

1. Navigate to the **Packet Forwarding page** on the Console Management Server.



2. Click the **Delete icon for the rule you want to delete**.
   A confirmation message appears.



3. Click **Delete**.

13 CryptoSync Configuration and Operation

13.1 CryptoSync Configuration

CryptoSync Settings

Use the **CryptoSync Settings** page to configure the amount of time before refreshing the authorization token and to enter the authorization token.

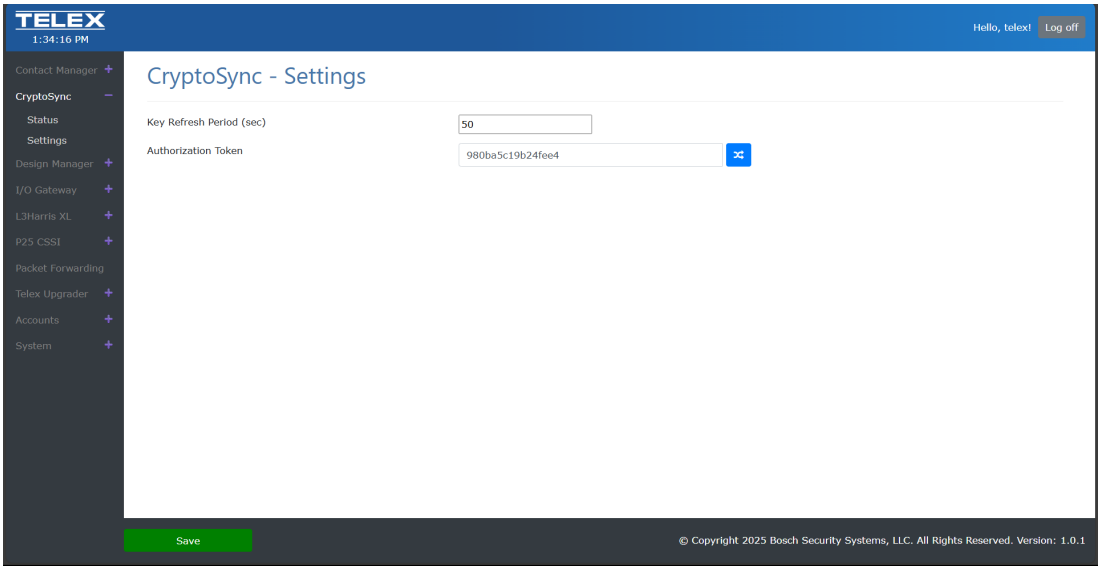


Figure 13.1: CryptoSync Settings Page

Key Refresh Period(s) Field

The **Key Refresh Period(s)** field defines the lifespan of keys generated and synchronized to CryptoSync clients.

The default value is 86400 seconds (24 hours).

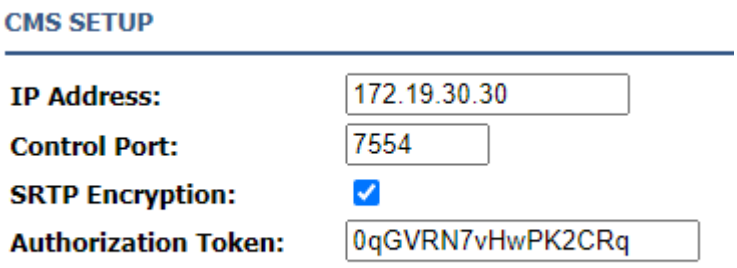
Authorization Token Field and Randomize Button

The **Authorization Token** field defines the authorization token used to validate the client. You can use your own authorization token or you can click the **Randomize** button to have CMS generate a new authorization token.

13.2 IP-224 Configuration

To **configure a connection to CMS-CryptoSync and SRTP Encryption on the IP-224**, do the following:

1. Login to **IP-224 website**.
2. Click on **Ethernet Setup**.
3. Navigate to the **CMS Setup**.



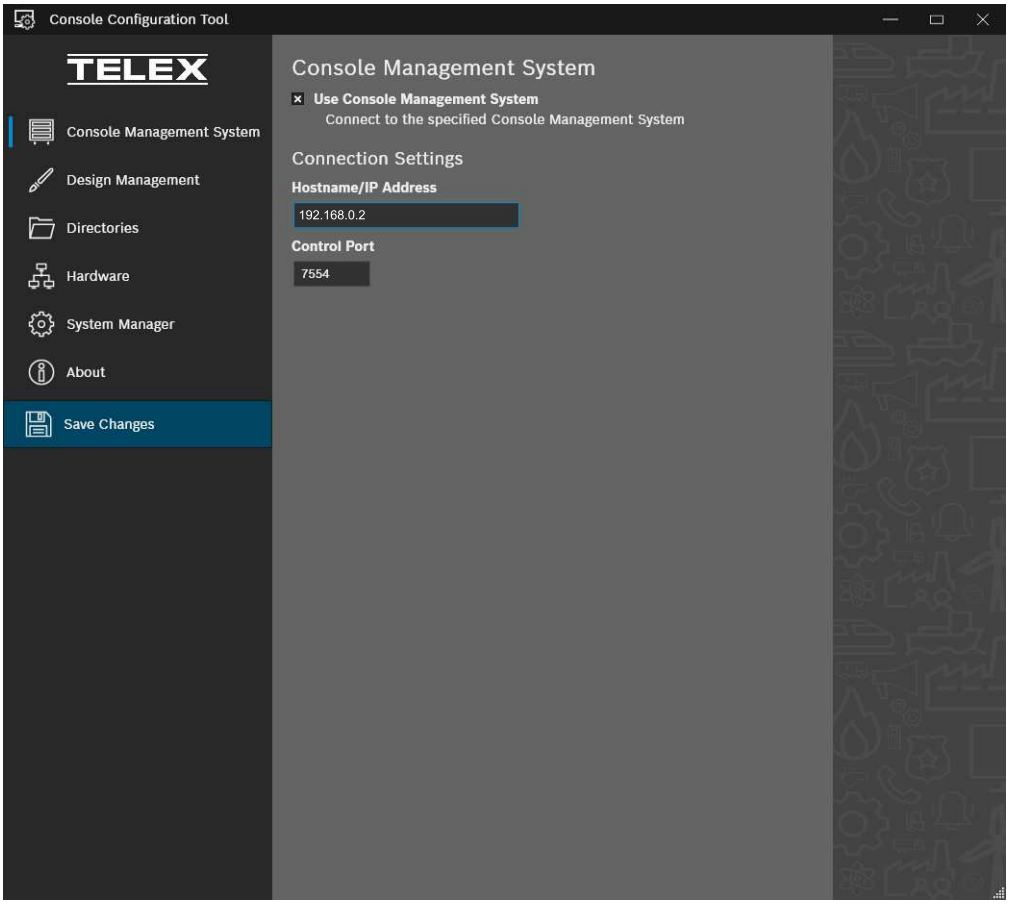
4. Enter the **IP Address** of the CMS workstation.
5. Enter the **Control Port** from Network Settings -> Design Management Port.
6. Select **sRTP Encryption check box.**
7. Enter the **Authorization token** from CryptoSync Settings.

13.3 C-Soft Configuration

13.3.1 Configure Connection to CMS

To **configure a dispatch position for CryptoSync**, do the following:

1. Open the **Console Configuration Tool**.
2. Navigate to the **Console Management System page**.



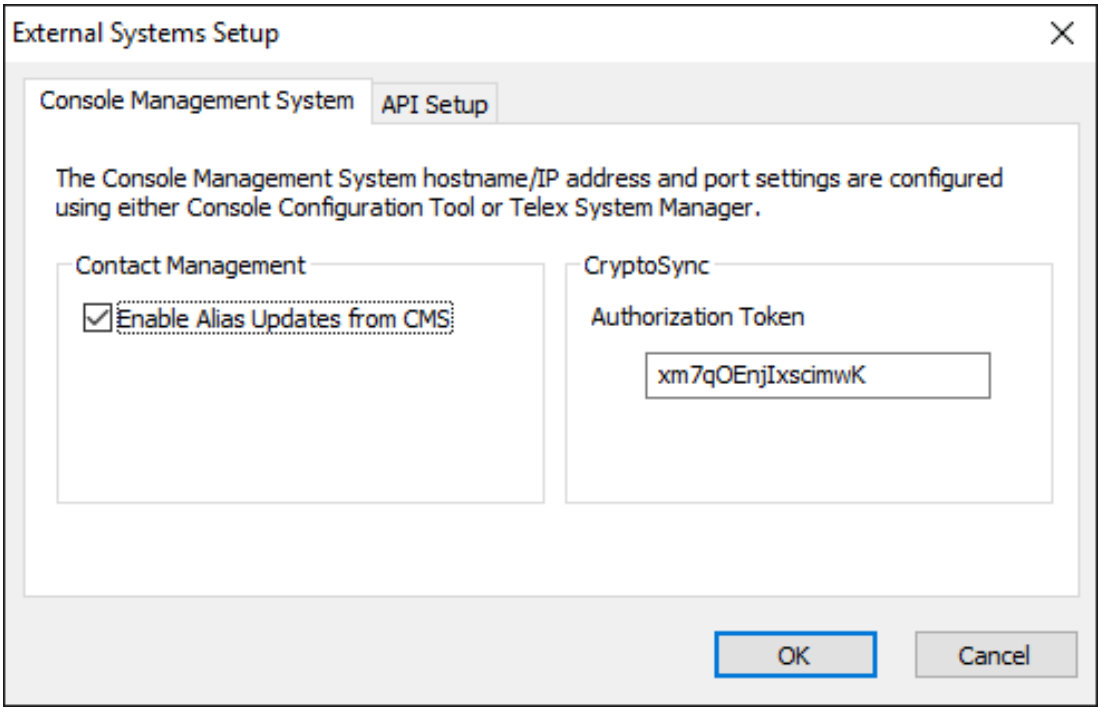
3. Select the **Use Console Management System check box**.
4. Enter the **Hostname or IP Address for CMS**.
5. Enter the **Control Port for CMS**.
6. Click **Save Changes**.

Notice!
If using CMS' Design Management or Contact Management features, these values have likely already been set. If configuring an IP-30XX, we recommend using TSM.

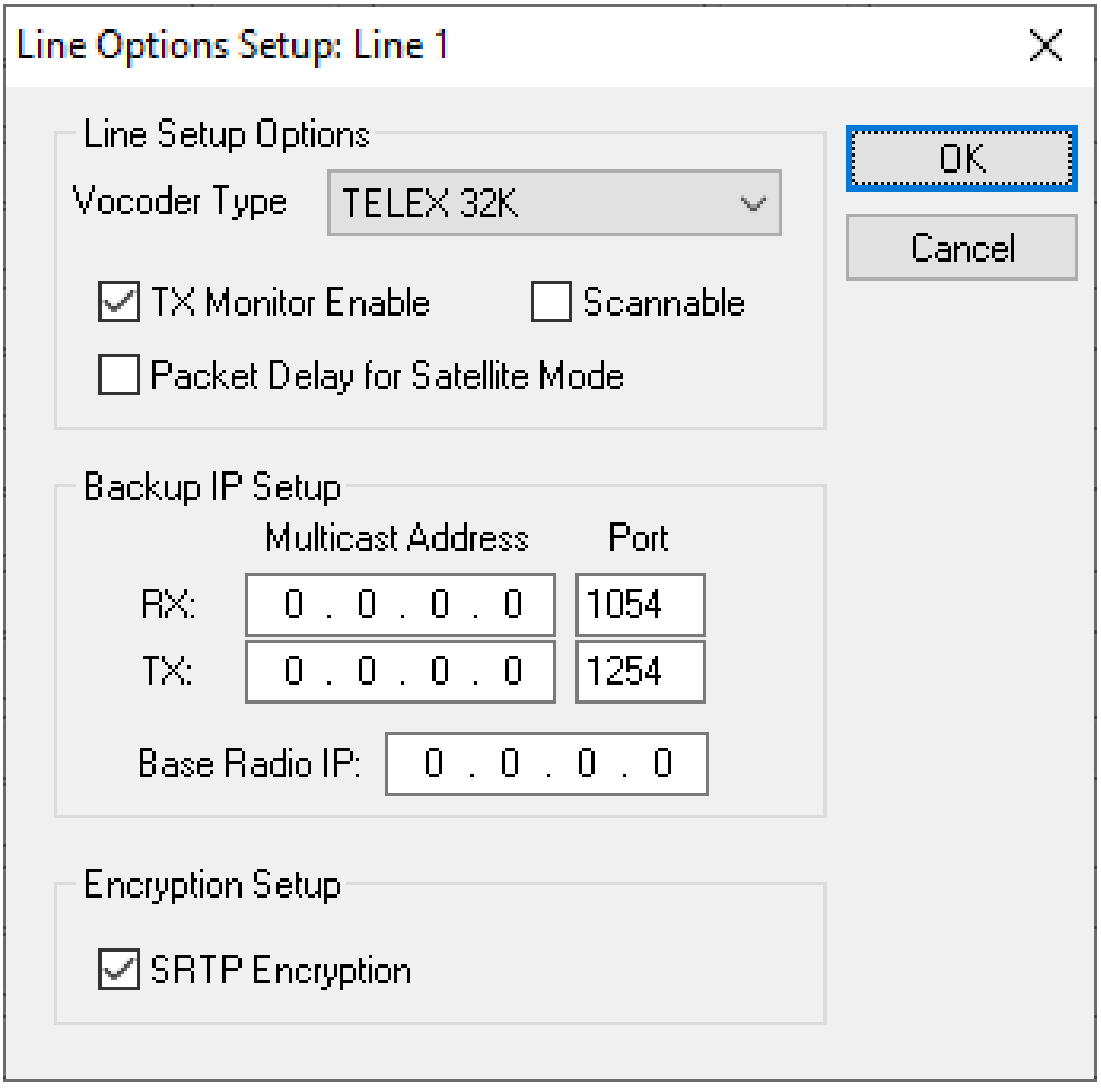
13.3.2 Configure C-Soft Design to use SRTP

To **configure a C-Soft design to use RSTP encryption for a given line**, do the following:

1. Open a **design** in C-Soft Designer.
2. Navigate to **Edit | Setup External Systems**.



3. Enter the **Authorization Token** from the CMS CryptoSync Settings page.
4. Click **OK**.
5. Navigate to **Edit | Setup Per Line Parameters**.
   The Per Line Parameters screen opens.
6. Click the **Options button** for the desired Telex line.
   The Line Options Setup screen opens.



7. Select the **SRTP Encryption check box**.
8. Press **OK**.
9. Repeat **steps 6 through 8**, as needed.

13.4 SRTP / CryptoSync Operation

While C-Soft Runtime and the IP-224 are running and are connected to CMS CryptoSync, they automatically acquire any cryptographic session keys and communicate them securely. No additional operational steps are necessary.

While transmitting or receiving a SRtp-secured call, C-Soft displays a “CRYPT” icon on the associated line’s Select button. A C-Soft, IP-224, or any other listener receiving a SRtp-secured call without access to CMS-CryptoSync is unable to decrypt the call and ignores the call.

CryptoSync Status

Use the **CryptoSync Status** page to monitor devices using CMS CryptoSync.

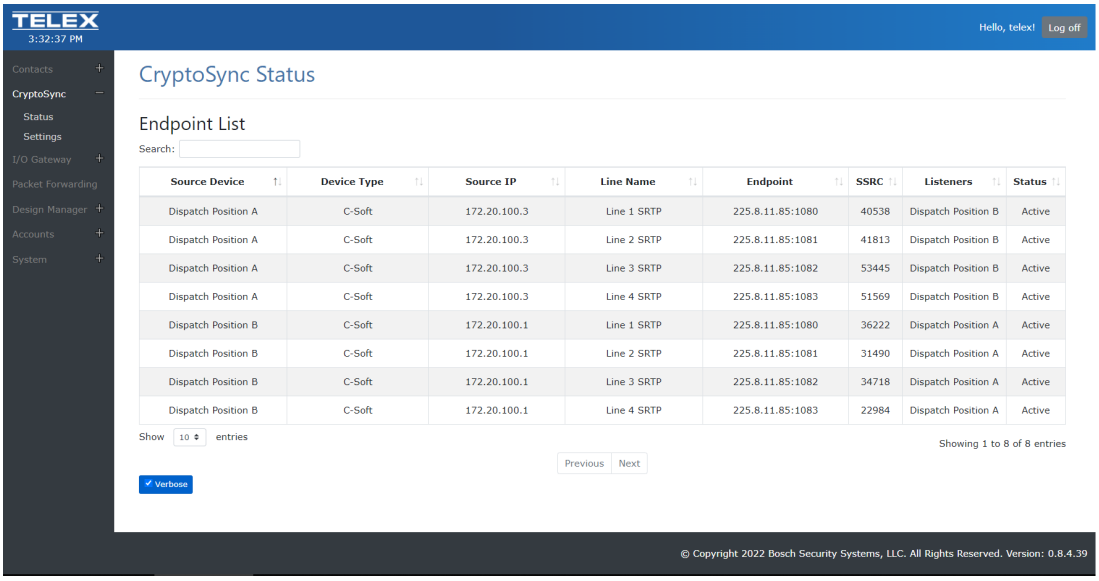


Figure 13.2: CryptoSync Status Page with the Verbose button enabled

Search Field

Use the **Search** field to quickly search for a specific source device in the list.

Source Device Field

The **Source Device** field displays the name of a specific device connected to CMS CryptoSync.

Device Type Field

The **Device Type** field displays the type of device connected to CMS CryptoSync.

Source IP Field

The **Source IP** field displays the IP address of the device subscribed to CMS CryptoSync

Line Name Field

The **Line Name** field displays the device's associated line name.

Endpoint Field

The **Endpoint** field displays the secure endpoint multicast address.

Verbose Button

Use the **Verbose** button to expand the number of columns available to monitor. The additional columns are: SSRC field, Listeners field, and Status field.

SSRC Field

The **SSRC** field displays the SSRC identifier for the device. This value is a 32-bit numeric identifier that is not dependent upon the network address.

Listeners Field

The **Listeners** field displays a list of listeners subscribed to the endpoint

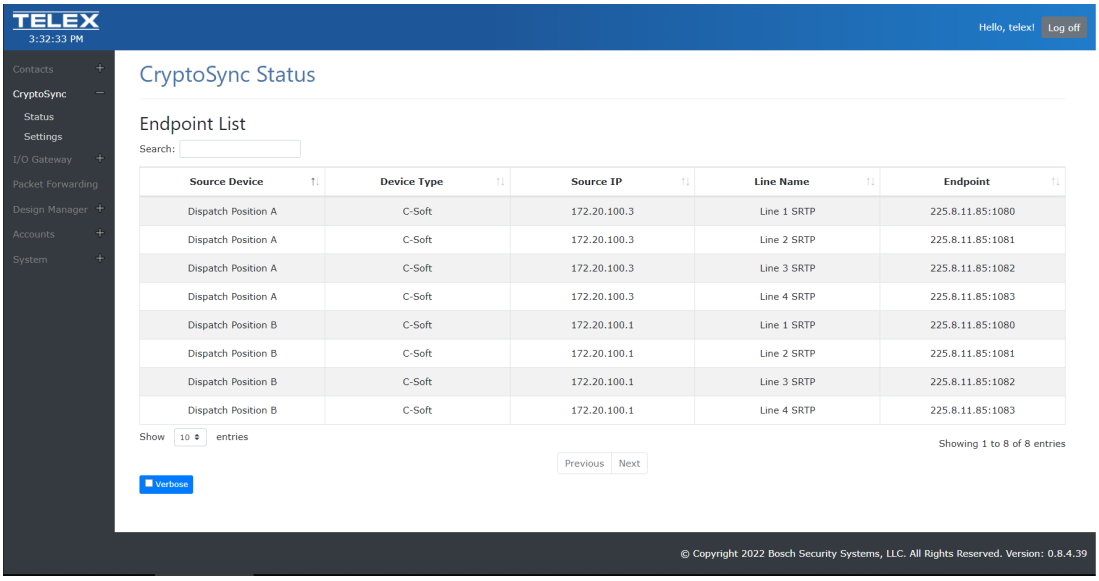
Status Field

The **Status** field displays the status of the CryptoSync connection.

During operation, CryptoSync client states can be monitored using the CMS CryptoSync Status Page.

To **monitor client states**, do the following:

1. Navigate to **CryptoSync | Status** in the left navigation.
   The CryptoSync Status screen appears. A list of all secure cryptographic transmitters endpoints is displayed. Each list entry identifies the source device's name subscribed to CryptoSync, its type, its address, the associated line's name, and finally the secure endpoint multicast address.



2. If desired, select the **Verbose check box** to also display the secure the sessions SSRC identifier. The SSRC identifier is a list of Listeners that are subscribed to the endpoint and the session's Status.

13.5 Telex Upgrader

The Console Management System added a new functionality to detect and remotely upgrade C-Soft software, IP-3XXX software, ADHB-4 Gen 2 firmware and IP-224 firmware. CMS is the central controller for Telex Radio Dispatch product line, it's only logical to add this functionality. Currently, this is only available using Telex System Manager (TSM). Each Telex Radio Dispatch product already contains all the necessary components that provide the ability to be remotely upgraded. These product components are beyond the scope of this document and this document will only focus on the CMS additions.

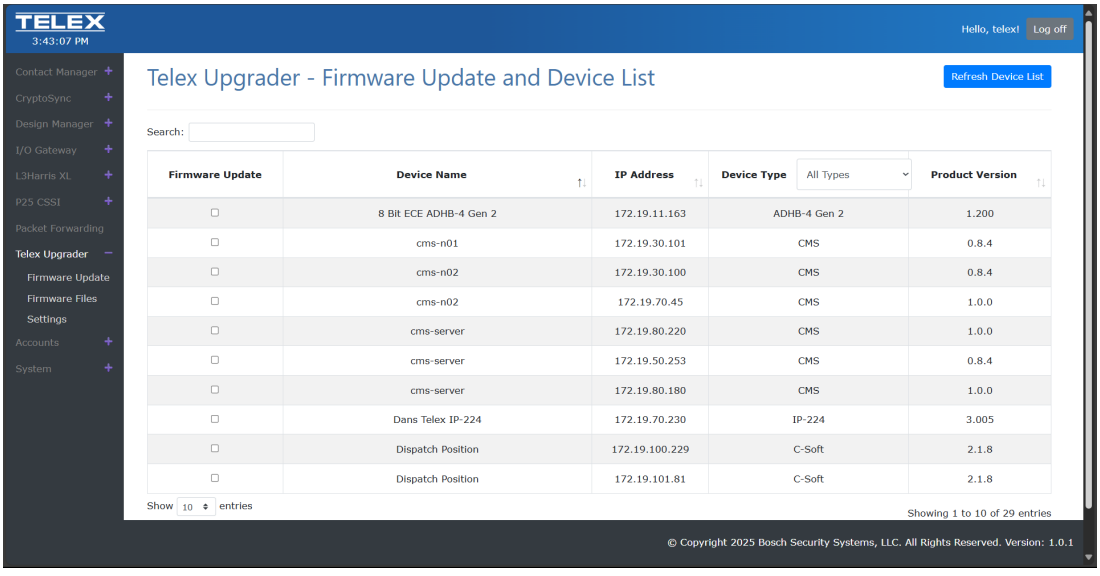


Figure 13.3: CMS Remote Product Upgrader - Device List

Firmware Update Checkbox

When checked allows the device to be upgraded.

Device name

Displays the name of the queried device.

IP Address

Displays the queried device's IP Address.

Device Type

Displays the queried device's product type. Either C-Soft, IP-3XXX, ADHB-4 Gen 2, or IP-224.

Device Type Dropdown Menu

Allows you to filter the device list to the selected Device Type.
You can filter by All, C-Soft, IP-3XXX, ADHB-4 Gen 2, or IP-224.

Product Version

Displays the device's current firmware/software.

Refresh Device List Button

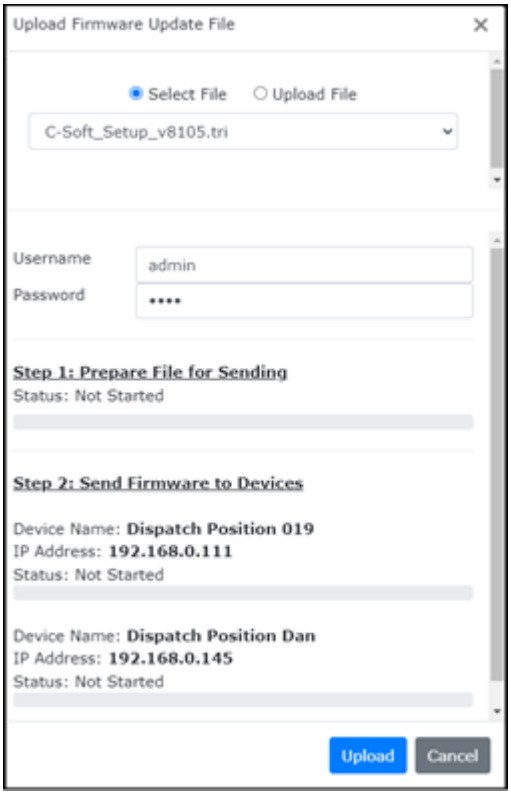
Clears the device list and sends out a network query to repopulate the device list.

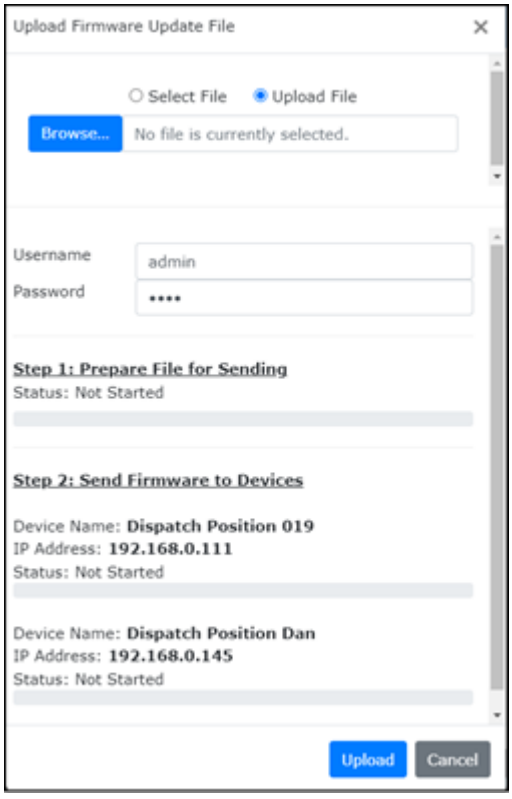
Search

The Search limits the device list to devices that contain the search term.

Upgrade Firmware button

Opens the Firmware Update window to allow the selected device(s) to be upgraded.





Select File radio buttons

When this radio button is selected, only firmware/software files that have already been uploaded to CMS can be selected and used to upgrade the device(s).

Upload File radio button

When selected, the firmware/software files are temporarily uploaded to CMS to upgrade the device(s).

Username
Displays the Username of the device(s) to be upgraded.

Password
The Password of the device(s) to be upgraded.

Step 1: Prepare File for Sending
Displays the progress for getting the firmware/software ready to send to the device(s).

Step 2: Firmware to Devices
Displays the progress for upgrading each device's firmware/software.

Upload button
Starts the firmware/software upgrade process.

Cancel button
Closes the firmware update window without upgrading the device(s).

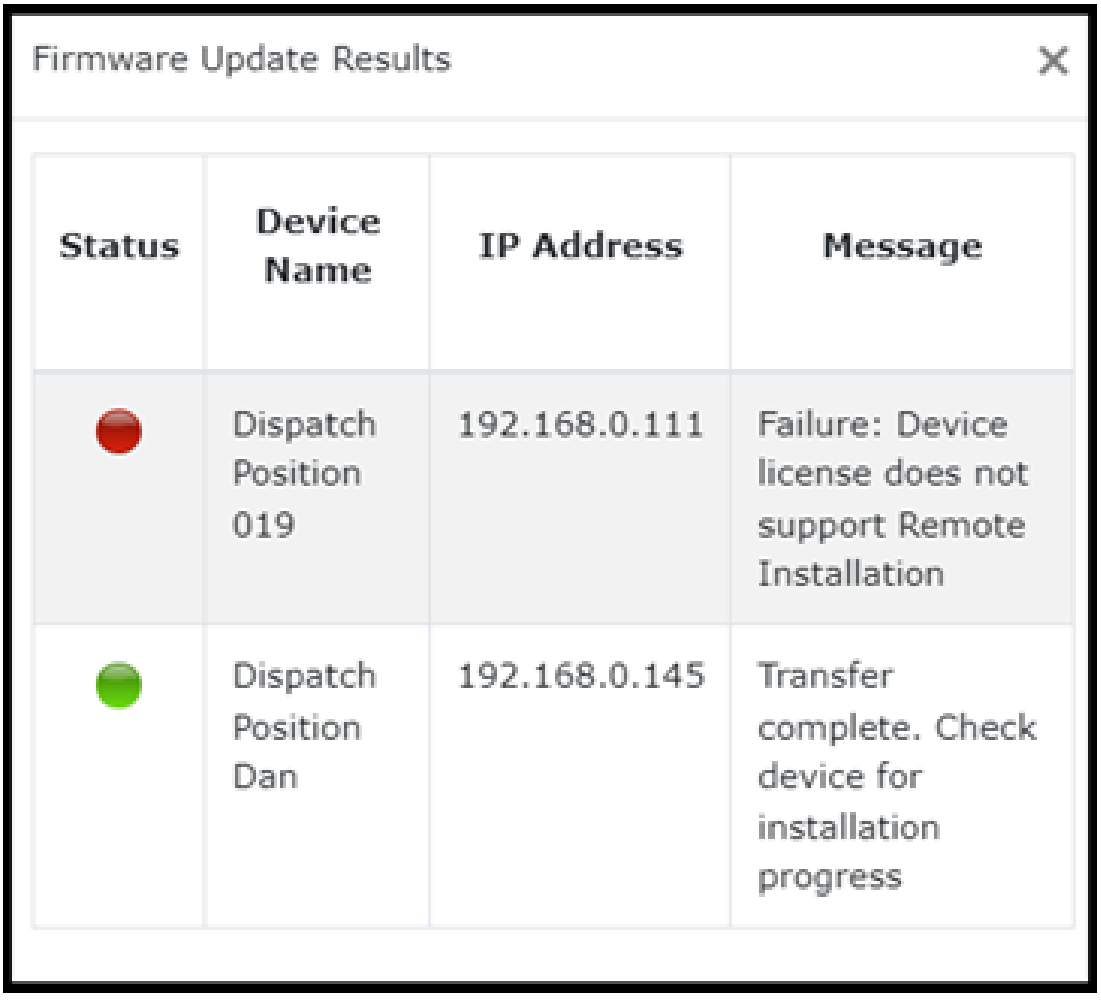


Figure 13.4: CMS Remote Product Upgrader - Firmware Update Results window

Status
Provides the upgrade status for each device.
Green indicates a successful upgrade.
Red indicates a failed upgrade.

Device Name
Displays the device name.

IP Address

Displays the device IP Address.

Message

Provides additional information about the upgrade status for each device.

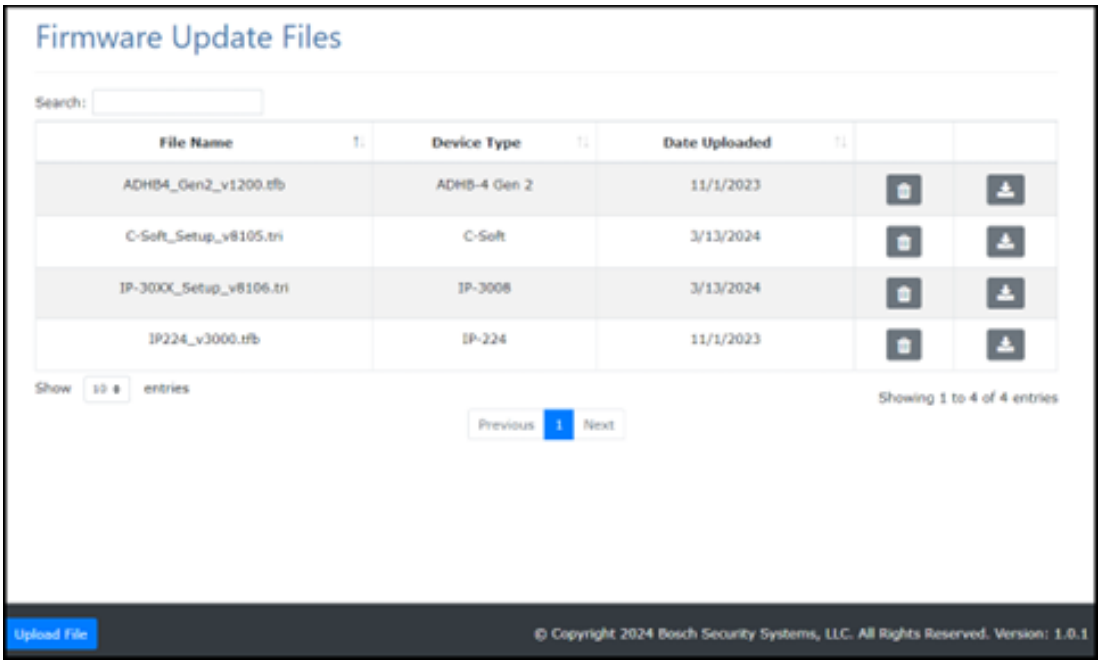


Figure 13.5: CMS Remote Product Upgrader - Files

File Name

Displays the file name of the firmware/software file that has been uploaded. Only file types of Telex Firmware Binary Files (*.tfb) or Telex Remote Installation (*.tri) are supported.

Design Type

Displays the file's device type. Either C-Soft(*.tri), IP-3XXX(*.tri), ADHB-4 Gen 2(*.tfb), or IP-224(*.tfb).

Date Uploaded

Displays the date the firmware/software file was uploaded.

Search

The Search limits the firmware/software list to firmware/software that contains the search term.

Trashcan icon button

Deletes the firmware/software file.

Download icon button

Downloads the firmware/software file.

Upload button

Opens the Upload Firmware File window.

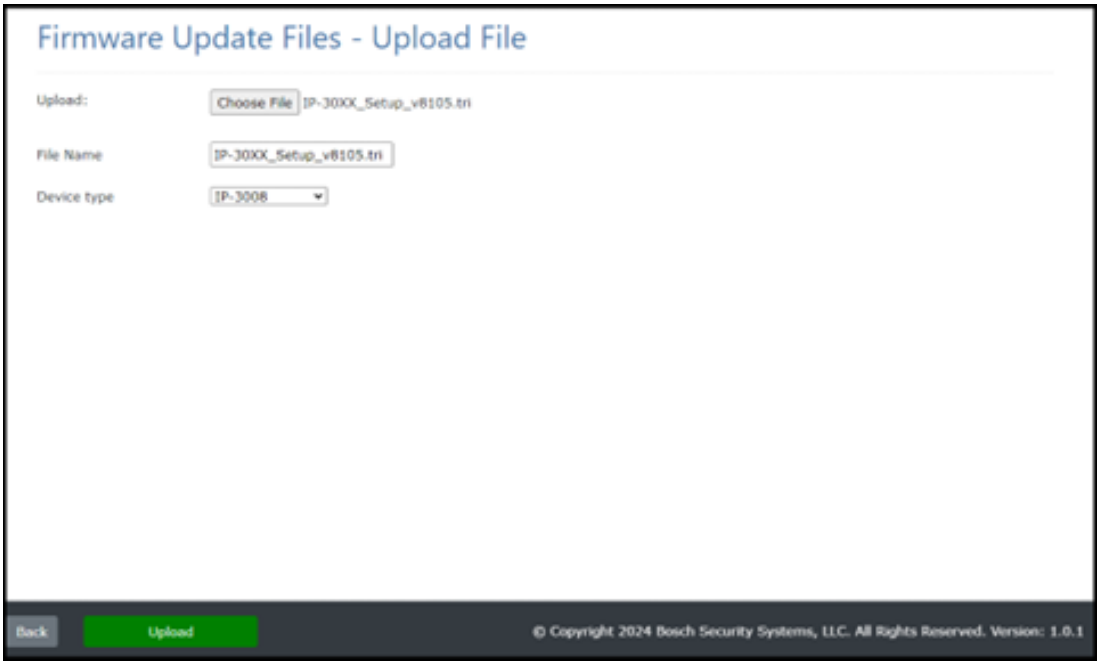


Figure 13.6: CMS Remote Product Upgrader - Upload File

Choose File button
Opens a window that allows you to browse for the desired firmware/software file.

File Name
Displays the file name of the firmware/software file to be uploaded. Only file types of Telex Firmware Binary Files (*.tfb) or Telex Remote Installation (*.tri) are supported.

Design Type
Displays the file's device type. Either C-Soft(*.tri), IP-3XXX(*.tri), ADHB-4 Gen 2(*.tfb), or IP-224(*.tfb) can be selected.

Back button
Returns to the Firmware Update File List page.

Upload button
Uploads the firmware/software file to CMS.

Multicast Ping IP Address
Specifies the multicast address on which Remote Product Upgrader sends a ping device query. Default is 233.15.18.22.

Multicast Ping Send Port
Specifies the port on which Remote Product Upgrader sends a ping device query. Default is 7635.

Multicast Ping Receive Port
Specifies the port on which Remote Product Upgrader receives ping device query replies. Default is 7636.

Multicast Ping TTL
Specifies the TTL for Remote Product Upgrader ping device query. Default is 10.

Device Detection Timeout
Specifies the maximum time to wait for ping device replies after sending a ping device query. Default is 500 ms.

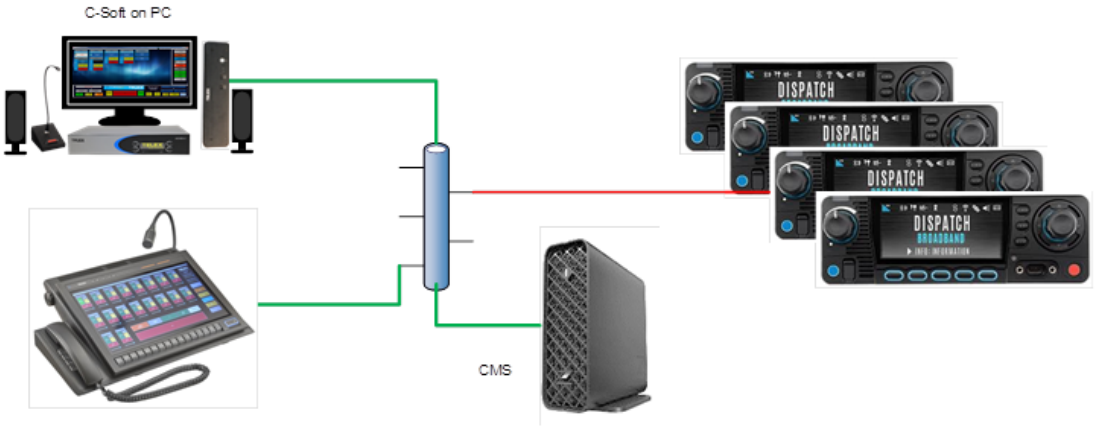
Firmware/Software Upgrade Timeout
Specifies the maximum time for a firmware/software upgrade. Default is 180 sec.

13.6 L3Harris XL

The Console Management System will be able to host connections to L3Harris XL radio using the XL Link feature in the radio, option is from Harris. CMS will support up to 20 L3Harris radio connections. Supported Features, Channel/TG change, ANI and EMER decode.

Product Licensing

- No additional licensing needed in C-Soft, uses standard available Telex line.
- CMS will require a XL license for each radio to be connected.
- XL connections can be ordered and added at any time using the following:



For additional information on configuration of CMS and L3Harris XL radio, please see our web site or contact tech support for our latest application note.

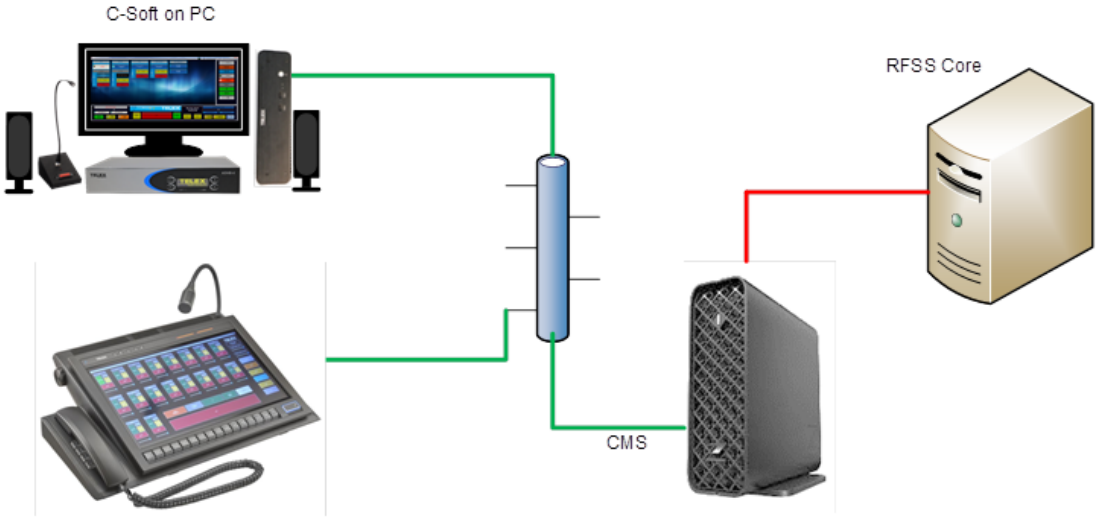
13.7 CSSI P25 Gateway

The Console Management System will be able to host connections to P25 Trunking systems using CSSI. CMS will support up to 100 Talk-Group registrations and 60 concurrent Talkpaths at once. Supported Features vary based on system, Channel/TG change, ANI and EMER decode standard.

Product Licensing

- Additional licensing is needed in C-Soft, uses CSSI line.
- CMS requires an Advanced license for each Talk-Group to be registered to in the system.

Advanced connections can be ordered at any time using the following:



For additional information on configuration of CMS and P25 Trunking systems, please see our web site or contact tech support for our latest application note.

14 Maintenance

15 Frequently Asked Questions

CMS Configuration

Question	Answer
What if the wrong IP information for the cluster is entered in the CMS Configuration?	Connect a monitor and keyboard to the units. Run the script `factoryreset.sh` found in /home/telex/utilities to rest the devices back to factory settings. Run the script by executing the following command: `sudo bash ~/utilities/factoryreset.sh` after logging in

System Management

Question	Answer
How do I check the status of the cluster?	Check the status of the cluster by accessing the terminal (either from SSH, Server Management page, or physically) and run the command `sudo pcs status`.
What if I forget my root password?	The root password is not resettable by the customer. The unit must be reset by our factory. If you still have access to the CMS server, it is recommended you back up any data you can before shipping the unit to the factory.
How can I download log files off CMS for help with Bosch Technical Support?	You can download all log files from the server from the *Log Settings, page 33* page.
Can I use my own SSL certificate?	Yes. Upload your SSL certificate under *SSL Certificate, page 33*.
How can I easily access the OS settings?	You can either ssh into the server using the account information set during configuration; or access CentOS's cockpit webpage from *System Status and Management, page 27* and then click the Server Management button located at the bottom of the page. Use the account information set during the configuration.
How do I revert the server to factory settings?	Perform a factory reset from the *System Status and Management, page 27*. Click the Factory Reset button located at the bottom of the page.
How do I upgrade CMS from and old version?	Obtain the latest CMS software (.cri file) from the Telex website (www.telex.com). Perform the upgrade from *System Status and Management, page 27*. Click the Upgrade CMS button located at the bottom of the page.
How do I turn off unused services in CMS?	Turn services off from the System Status/Manage page. Click stop of each of the services you do not want to run. Turning off the services is not persistent and the services will start again, when the server is restarted, upgraded, or factory reset.

Contact Management

Question	Answer
Why can't I change an alias and an ID at the same time?	Due to system limitations, it is not possible to change both an alias and an ID at the same time. You can achieve this goal by editing the alias first and the ID second.
Can I automate importing cvs/system lists?	While it is possible to automate importing contacts, we do not recommend this due to soft deletes. Over time, frequent imports can cause the database to grow very large.
Are fleets supported in FleetSync?	No, while a FleetSync alias type is supported, the support for fleets is not.

CryptoSync

Question	Answer
Why does C-Soft decode encrypted packets even when the line is not configured for SRTP Encryption?	The Per-Line SRTP Encryption check box defines C-Soft's transmit behavior. If CryptoSync is otherwise configured (CMS Connection parameters set through Console Configuration Tool, and CryptoSync Authorization Token is set in design), C-Soft attempts to retrieve cryptographic contexts and decrypt the play audio. This matches other C-Soft settings behavior (i.e., P25-DFSI Encryption, Vocoder settings)
I am using Packet Forwarding and CryptoSync, and C-Soft is not decrypting the forwarded audio stream.	CryptoSync only works with audio streams originating from C-Soft or IP-224. If a secure audio packet rebroadcasts to a different multicast endpoint, C-Soft is unable to identify the cryptographic parameters for that stream, and is unable to obtain cryptographic parameters needed to decode it.

I/O Gateway

Question	Answer
Can I use my own MQTT broker?	Yes, you can change the MQTT broker connection information on the I/O Gateway Settings page of the CMS.
Can I use my SSL with my own MQTT broker?	Yes, you need the valid certificate authority. Be sure to name the certificate to ca.crt and copy it to /etc/opt/telex/cms/ on the CMS server.
Why do I have issues with I/O Gateway on multiple network adapters?	I/O Gateway is not supported for use with multiple network adapters. We recommend a single network connection if you are using the I/O Gateway.
Why does C-Soft Runtime display "Error Setting Relay" after pressing a Relay Control button configured to use MQTT?	This error message in C-Soft Runtime generally indicates the ADAM device is either not connected or unable to connect to the MQTT broker. Check the MQTT broker settings on the ADAM and then restart the ADAM device.

Question	Answer
What IP Address should I use when configuring the Relay Control and Input Indication buttons in C-Soft Runtime?	The IP address of the CMS PC should be used. C-Soft Runtime is connecting to the CMS PC and therefore requires the CMS PC's IP address.

Packet Forwarding

Question	Answer
Why am I having issues using packet forwarding with multiple network adapters?	Packet forwarding is not supported for use with multiple network adapters. We recommend a single network connection if you are going to use packet forwarding.

Design Manager

Question	Answer
How can I easily view what designs users are assigned?	You can view overall user design assignments from the *Design Manager Configuration and Operation, page 40* page.

Account Management

Question	Answer
Why can a dispatcher rights only role not login to the website?	Due to security risks, non-administrator accounts cannot access the website. If you would like a role to have access/limited access to the webpage, you must change the role to have administrator rights and then specify which sections of the website they can access.
I forgot all my CMS administrator account passwords, how do I reset them?	You need to access the terminal (either from SSH, Server Management page, or physically), and then run the `factoryreset.sh` script in /home/telex/utilities to reset the devices back to factory settings. You can run the script by executing the following command: `sudo bash ~/utilities/factoryreset.sh` after logging in.

C-Soft

Question	Answer
Can I use Console Launcher over a window's remote desktop connection?	No, due to limitations with windows remote desktop connection, Console Launcher cannot be used. C-Soft can still be used by accessing csoftruntime.exe in C:\Program Files (x86)\Telex Communications\C-Soft.

Question	Answer
I am getting a license error for CMS in C-Soft, what is this?	This means you are consuming all of your CMS licenses. You can check the status of active connections in *System Status and Management, page 27* and your current connections licenses in *Licensing, page 37*.

16 Technical data

Electrical

Power supply	180 Watt Smart PFC Slim Straight AC Adapter
Supply voltage	100-240 VAC, 50-60 Hz
Rated input current	2.5 A @ 90 VAC (180 Watt Smart PFC Slim Straight AC Adapter)
ENERGY STAR certified	Yes
FEMP standby power compliant	Yes, with Wake-on-LAN disabled
Surge tolerant full ranging power supply (withstands power surges up to 2000V)	Yes

Mechanical

Dimensions (H x W x D)	2.7 in. x 8.3 in. x 8.6 in. (6.9 cm x 21.1 cm x 21.8 cm)
Weight	5.3 lbs (2.4 kg)
Box Dimensions	19.5 in. x 6.25 in. x 11.5 in. (495.3 mm x 158.75 mm x 292.10 mm)
Boxed Weight	7.95 lbs. (3.60 kg)

Environmental

	TCMS-P Console Management System Package
Operating temperature (°F)	40 °F – 95 °F (5 °C - 35 °C)
Storage temperature (°F)	-40 °F – 140 °F (-40 °C - 60 °C)
Operating relative humidity, non-condensing (%)	10% – 85%

*Above 1524 m (5.000 ft.) altitude, the maximum operating temperature is reduced by 1 °C (1.8 °F) for every 305 m (1.000 ft.) increase in elevation.

Bosch Security Systems, LLC
130 Perinton Parkway
Fairport, NY 14450
USA
www.telex.com

EU importer:
Bosch Sicherheitssysteme GmbH
Robert-Bosch-Platz 1
70839 Gerlingen
Germany

202508151629