

Console Management System

TCMS - Console Management System



en Technical Manual

Table of contents

1	Notices	5
1.1	Proprietary notice	5
1.2	Copyright notice	5
1.3	Warranty notice (limited)	5
1.4	Factory service center	5
1.5	Contact information	5
1.6	Claims	5
1.7	Warning	6
1.8	PC & Network Security consideration	6
2	Introduction	7
3	System overview	8
4	Quick Installation	9
5	Logging In	15
5.1	Initial Login	15
5.2	Home page	16
6	Account Management	17
6.1	Manage Users	17
6.1.1	Create Users	18
6.1.2	Edit Users	19
6.2	Manage Roles	21
6.2.1	Create Role	22
7	System Management Operation	24
7.1	System Status and Management	24
7.1.1	Service Status	24
7.1.2	Console Connection Status	25
7.1.3	Upgrade CMS	25
7.1.4	Restart Server	25
7.1.5	Shutdown Server	26
7.1.6	Factory Reset	27
7.1.7	Server Management	27
7.2	Network Settings	27
7.3	Log Settings	28
7.4	SSL Certificate	29
7.4.1	Install a SSL certificate file manually	30
7.4.2	Generate a custom SSL certificate using CMS	31
7.4.3	Display the current installed Private Key and Installed Certificate	32
7.5	Licensing	33
7.5.1	Create a capability request	34
7.5.2	Deploy a capability response	35
7.6	About CMS	36
8	Design Manager Configuration and Operation	37
8.1	User/Role Creation	37
8.2	CMS Design Repository	37
8.2.1	Create TDA Files	37
8.2.2	Upload Designs	37
8.2.3	Manage Uploaded Designs	38
8.3	C-Soft/CMS Connection Configuration	40
8.3.1	Configure Connection to CMS	41

8.4	Configure Design Manager	42
8.5	C-Soft Launch Operation	43
9	Contact Management and Operation	45
9.1	Dispatch Position Setup	45
9.1.1	Configure Connection to CMS	45
9.1.2	CMS Alias Updates for the Design	45
9.2	Contact Overview	46
9.2.1	Search	50
9.2.2	Import CSV	50
9.2.3	Export CSV	51
9.2.4	Import System List	52
9.2.5	Save	53
10	I/O Gateway Configuration and Operation	54
10.1	Broker Settings Page	55
10.2	Device Settings Page	56
10.3	ADAM-6000 Series Configuration	57
10.3.1	Hardware Setup	57
10.4	TLS Operation	57
10.4.1	Configure the Mosquitto Broker	57
10.4.2	Enable TLS in CMS	58
10.5	User Name and Password Operation	58
10.5.1	Mosquito Broker Configuration	59
10.5.2	Console Management System Configuration	59
10.5.3	ADAM-6000 Series Configuration	60
11	Packet Forwarding Configuration and Operation	62
11.1	Edit Rule	62
11.2	Add Rule	66
11.3	Copy Rule	68
11.4	Delete Rule	71
12	CryptoSync Configuration and Operation	73
12.1	CryptoSync Configuration	73
12.2	IP-224 Configuration	73
12.3	C-Soft Configuration	74
12.3.1	Configure Connection to CMS	74
12.3.2	Configure C-Soft Design to use SRTP	75
12.4	SRTP / CryptoSync Operation	76
13	Frequently Asked Questions	79
14	Technical data	83

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

Copyright 2022 by Bosch Security Systems, LLC. All rights reserved. Reproduction, in whole or in part, without prior written permission from Bosch is prohibited. *All other trademarks are property of their respective owners.

1.3 Warranty notice (limited)

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

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@us.bosch.com Phone: (800) 752-7560 Fax: (402) 467-3279

Customer service repair

E-mail: repair@us.bosch.com Phone: (800) 553-5992

Technical support

E-mail: TelexDispatchtechsupport@us.bosch.com Knowledge database: http://knowledge.boschsecurity.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.

i

Notice!

Bosch 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.

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-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.

3 System overview



2024-03 | V04 | F.01U.404.075

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.

letwork Connection Details	
Property	Value
Connection specific DN	
Description	Intel(R) I210 Gigabit Network Connection
Physical Address	00-22-4D-D6-89-47
DHCP Enabled	Yes
Autoconfiguration IPv4	169.254.37.48
IPv4 Subnet Mask	255.255.0.0
IPv4 Default Gateway	
IPv4 DNS Server	
IPv4 WINS Server	
NetBIOS over Topip En	Yes
Link-local IPv6 Address IPv6 Default Gateway	fe80:5522:2291:e955:2530%9
IPv6 DNS Servers	fec0:0:0#ff::1%1
	fec0:0:0:0##f::2%1
	fec0:0:0##:3%1
¢	,

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.

í

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.

CMS Configuration

Configuration

Using Failover

Linux Root Password

Confirm Linux Root Password

Linux User Password

Confirm Linux User Password

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.

Network Adapter Status

eno1 : Down

ens3f0u1 : Up

Please select a network adapter

Network Adapter

ens3f0u1 ♥

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.

IP Address

Subnet		
Gateway		
DNS Server		

Enable IPv6

1	1	
	-	

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.

i

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.

□ Is Primary Server

Other server node IP Address

Cluster IP Address

Other server node root password



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.

v

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

Use NTP

Timezone

(UTC-06:00) Central Time (US & Canada)(Central Standard Time)	
---	--

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).

Cor	nfirm Settings		×
	Root Password: ••••	۲	
	Telex Password: ••••	۲	
	Network Adapter: Ethernet		
	IP Address: 172.19.100.11		
	Subnet: 255.255.0.0		
	Gateway: 172.19.100.168		
	DNS: 1.1.1.1		
	NTP Active: true		
	Timezone: Central Standard Time		
	Gateway: 172.19.100.168 DNS: 1.1.1.1 NTP Active: true Timezone: Central Standard Time		



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

Property	Value
Connection-specific DN	localdomain
Description	Intel(R) I210 Gigabit Network Connection
Physical Address	0C-C4-7A-83-09-1D
DHCP Enabled	No
IPv4 Address	172.19.20.80
IPv4 Subnet Mask	255.255.0.0
IPv4 Default Gateway	172.19.100.168
IPv4 DNS Servers	4.4.4
	8.8.8.8
IPv4 WINS Server	
NetBIOS over Topip En	Yes
IPv6 Address	fd98:2aec:a4d0.f7dc::1236
Link-local IPv6 Address	fe80::2c16.6e09.19c8;d724%2
IPv6 Default Gateway	fd98:2aec;a4d0:f7dc::1
IPv6 DNS Server	
¢	,

- 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.

CMS Configuration

CMS Configuration is now complete!

Please connect to your network and access with the link below

https://10.2.3.86



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. Please refer to the License Installation Instructions for further information.

5 Logging In

5.1 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.

TELEX 1:04:20 PM	
	Login
	Use a local account to log in.
	Usemame Telex
	Password
	Log in
	© Copyright 2022 Bosch Security Systems, LLC. All Rights Reserved. Version: 0.7.2

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

Set Password.

Please change the default password.

		(A)	
Confirm	new pass	word	

6. Enter your **new password**.

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

5.2 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.

2:37:43 PM				8	Hello, Telex!	Log off
	Console Manageme	nt Syste	em			
	CONTACTS Edit user and group contact aliases	222	CRYPTOSYNC Configure audio encryption settings	8		
	I/O GATEWAY Configure MQTT devices	\mathbf{X}	PACKET FORWARDING Set up rules for packet forwarding	۲ 1		
	DESIGN MANAGER Upload TDA files for management		ACCOUNTS Manage system users			
	SYSTEM Manage the Console Management System					
		© Copy	right 2022 Bosch Security Systems, LLC	. All Rights Rese	rved. Version	: 0.8.4.38

6

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.

6.1 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.

Contacts + CryptoSyrc + YO Gateway + Packet forwarding earonson Design Manager + Administrator Accounts - bbrown Police Bill Brown Contacts -	
L/O Gateway + Packet Forwarding - Design Manager + - bbrown - Accounts - Image: Packet Forwarding	
Packet Forwarding Design Manager + aaronson Administrator Aaron Aaronson C C Accounts - bbrown Police Bill Brown C C C	
Accounts - bbrown Police Bill Brown Cr	
Manage Users Manage Roles Fire Candice Crowe Crowe	
System + ddavis EMT Donald Davis 2	
eevans Administrator Eric Evans 7	
ffreeman Police Francine Freeman <table-cell></table-cell>	
ggardner Police Gordon Gardner 📝	
Create User © Copyright 2022 Bosch Security Systems, LLC. All Rights Reserved. Version: C	1.8.4.39

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 21*.

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 18.*

To edit a user profile, see Edit Users, page 19.

6.1.1 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.

2:16:25 PM		Hello, Telex!	Log off
Contacts + CryptoSync +	Create User		
CryptoSync + I/O Gateway + Packet Forwarding Design Manager + Accounts - Manage Users Manage Roles System +	Username		
	Back to All Users Save		

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 21*.

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.

6.1.2 Edit Users

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

2:24:12 PM				Hello, Telex!	Log off
Contacts + CryptoSync + I/O Gateway +	Manage U telex (telex telex	ser)			
Packet Forwarding	Username	telex			
Design Manager +	Password	******			
Accounts –	PIN (optional)	#####			
Manage Roles	First Name	telex			
System +	Last Name	telex			
			C	5	
	Back to All Users	Save			

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:

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

6.2 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.

2:30:30 PM				Hello, Telex! Log off
Contacts + CryptoSync +	Manage Roles			
I/O Gateway 🕂	Role	Туре		
Packet Forwarding	Administrator	Administrator	6	
Design Manager +	Dispatcher	Dispatcher	1	
Accounts —	•		L B	
Manage Users				
System +				
	Create Role	© Copyright 2022 Bosch Security Sys	stems, LLC. All Rights Re	eserved. Version: 0.8.4.38

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.

6.2.1 Create Role

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

TELEX 12:39:21 PM		Hello, Telex!	Log off
Contacts +	Create Role		
I/O Gateway +	Role Name		
Design Manager + Accounts - Manage Users Manage Roles System +	 Administrator Rights Contact Management Rights Packet Fowarding Rights I/O Gateway Rights CryptoSync Rights TDA File Manager Rights 		
	Back to All Roles		

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.

Packet Forwarding Rights Check Box

The **Packet-Forwarding Rights** check box enables packet-forwarding 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.

CryptoSync Rights Check Box

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

TDA File Manager Rights Check Box

The **TDA File Manager Rights** check box enables TDA file manager rights to the role.

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.

7 System Management Operation

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

7.1 System Status and Management

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

7.1.1 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.

+ 10 +	System State	us an	d Ma	nager	nent			
av +	Server Hostname:	c <mark>m</mark> s-se	rver					
warding nager	Service Status							
+	Service Name	Status						
	Contact Management		Start	Stop				
age	CryptoSync		Start	Stop				
1	I/O Gateway		Start	Stop				
3	Packet Forwarding		Start	Stop				
	Design Manager		Start	Stop				
	Console Connects	ction S	Status	Sourc	e Device IP	11	Active Connections	Ť
				No data	available in tab	le		

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.

7.1.2 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.

7.1.3 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.

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

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

The Upgrade CMS window opens.

FX						
1 PM	Upgrade CMS				×	Hello, Telex! Log of
+	Upload CMS .cri File:	Browso	No filo col	octod		
nc +		biowse	NO THE SER	ecceu.		
vay +			Upgrade	CMS Serve	Close	
rwarding	Service Status	_				
anager	Service Status					
+	Service Name	Status				
_	Contact Management		Start	Stop		
Manage			June	Stop		
	CryptoSync		Start	Stop		
inac	I/O Gateway		Start	Stop		
ings						
g	Packet Forwarding		Start	Stop		
1S	Design Manager		Start	Stop		
	Console Conne	ction St	atus			
	console conne	ction st	atas			
	Search:					
	Source Device	e †		Source De	vice IP	Active Connections
			1	lo data avai	able in table	
	Show 10 + entries		1	lo data avai	able in table	Showing 0 to 0 of 0 entries

- 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.

7.1.4 Restart Server

To restart the entire CMS server, do the following:

1. Click **Restart Server**.

A Restart Server confirmation message appears.

TELEX 1:32:00 PM	Restart Server X Hello, Telex Log off
Contacts +	Are you sure you want to restart the server?
CryptoSync + I/O Gateway +	Yes No
Packet Forwarding	Service Status
Accounts +	Service Name Status
System –	Contact Management Start Stop
Status/Manage Network	CryptoSync Start Stop
Settings Log Settings	I/O Gateway Start Stop
SSL Settings Licensing	Packet Forwarding Start Stop
About CMS	Design Manager Start Stop
	Console Connection Status
	Search:
	Source Device 1 Source Device IP 11 Active Connections 11
	No data available in table
	Show 10 ¢ entries Showing 0 to 0 of 0 entries
	Upgrade CMS Restart Server Shutdown Server Factory Reset Server Management

2. Click Yes.

7.1.5 Shutdown Server

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

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

1:31:50 PM Shutdown Server antacts + CyptoSync + Service Name Status crket Forwarding Contact Management Statt ccounts + CryptoSync • Image: + Contact Management Statt ccounts + V/O Gateway • Start status/Manage Packet Forwarding Start Network Settings Packet Forwarding Start SSL Settings TDA File Manager Start Are you sure you want to shutdown the Start Are you sure you want to shutdown the •	TELEY					
antacts + ryptoSync + G Gateway + acket Forwarding counts + ystem - Status/Manage + Network Settings SL Settings - Licensing - DA File Manager - Status - TDA File Manager - Status -	1:31:50 PM			Shutdown	Server	
rypto Symc + O Gateway + icket Forwarding esign Manager + coounts + Status/Manage Network Settings Status/Manage Network Settings TDA File Manager = Status Stop		System Sta	tus and N	Are you si	re you want to shutd	own the server?
O Gateway + acket Farwarding Contact Management esign Manager + ccounts + Status/Manage CryptoSync Status/Manage J/O Gateway Network Settings Packet Forwarding SSL Settings TDA File Manager About CMS TDA File Manager		System Sta				
acket Forwarding esign Manager + ccounts + Status/Manage Status/Manage CryptoSync © Start Stop 1/O Gateway © Start Stop Network Settings SSL Settings Licensing TDA File Manager © Start Stop		Service Name	Status			
esign Manager + CryptoSync Start Stop ystem - Status/Manage Packet Forwarding Start Stop Licensing TDA File Manager Start Stop		Contact Managaman				
counts + CryptoSync Start Stop stem - 1/0 Gateway Start Stop Status/Manage Packet Forwarding Start Stop SSL Settings Packet Forwarding Start Stop SSL Settings TDA File Manager Start Stop		Contact Managemen	Stai	Stop		
Astern - Status/Manage Network Settings SSL Settings Licensing Dacket Forwarding TDA File Manager Dacket Start Start Start Start Stop		CryptoSync	Stal	Stop		
Status/Manage Pocket Forwarding Start Stop Network Settings Packet Forwarding Start Stop SSL Settings TDA File Manager Start Stop About CMS Start Stop		1/O Gateway				
Network Settings Packet Forwarding Start Stop SSL Settings TDA File Manager Start Stop		1/O Gateway	Star	Stop		
SSL Settings Licensing TDA File Manager Start Stop		Packet Forwarding	Stat	tStop		
About CMS		TDA File Manager				
		TOA Lie Manager	Stal	Stop		
				lown Server		
Upgrade CM5 Restart Server Shutdown Server Factory Reset Server Management				Las		

2. Click Yes.

The entire CMS server is shut down.

7.1.6 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.

Factory Reset	×
Are you sure you want to factory reset the server?	
□ Would you like to delete the database?	
Yes	No
2 Select the Would you like to delete the detabase shock her, if applicable	

2. Select the Would you like to delete the database check box, if applicable.

 Click Yes. The Server resets to its factory default settings.

7.1.7 Server Management

7.2 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 12:11:42 PM		Hello, Telex! Log off
Contacts + CryptoSync +	Network Settin	gs
I/O Gateway + Packet Forwarding	Global Port Settings	
Design Manager +	Control Port 7554	
Accounts +	Alias Management Port	
System —	5988	
Status/Manage	CryptoSync Port	
Network Settings	6167	
Log Settings		
SSL Settings		
Licensing		
About CMS		
	Save	© Copyright 2022 Bosch Security Systems, LLC. All Rights Reserved. Version: 0.8.4.38

Control Port Field

Use the **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.

Alias Management Port Field

Use the Alias Management Port field to enter the port used for alias management.

CryptoSync Port Field

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

7.3 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:

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

.32 PM			Hello, Telexi	
ts + Sync +	System Log S	Settings		
teway +	Log Folder Size: 1.7G			
Forwarding	Service Name	Log Level		
Manager +	Web Server (Telex)	Debug v		
its +	Web Server (Microsoft)	Information ~		
n —	Contact Management	Warning v		
us/Manage	CryptoSync	Warning v		
ngs	I/O Gateway	Warning v		
Settings Settings	Packet Forwarding	Warning v		
nsing	Design Manager	Warning v		
it CMS				

- 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.

7.4 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

7.4.1 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.

7.4.2 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.

Generate Custom Certificate

Domain Name:	
Organization Name:	
Organization Unit:	
Country Name (2 Letter Code):	
State/Province (Full Name):	
City(Full Name):	

3. Enter the following information:

Cancel

Submit

X

- 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.

Install Signed Certificate

×



- 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.

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.
- Click Display Private Key, Installed Certificate. The Installed Key and Certificate screen opens with the current private key and certificate fields populated.

7.4.3

Installed Key and Certificate	\searrow	×
Private Key:	BEGIN PRIVATE KEY MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAo BAQDD6MQuOdfYtidm tpvfC9KgzyjvicEaPvcWcnh3gWKSctuqsYSJyj43Nb5CBF92i AI6lw3lAIZY4EMa pvCGoONmOff0As37iyC27p7H7slPevM4RShW61+iffHwXP	
Signed Certificate:	BEGIN CERTIFICATE MIIDnzCCAoegAwIBAgIJAOkMFm8V9zIYMA0GCSqGSIb3D QEBCwUAMGYxCzAJBgNV BAYTAIVTMREwDwYDVQQIDAhORUJSQVNLQTEQMA4GA1U EBwwHTEIOQ09MTjEOMAwG A1UECgwFQk9TQ0gxDjAMBgNVBAsMBVRFTEVYMRIwEAYD	< >//:

Cancel

7.5 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



7.5.1 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.

Generate Capability Request

×



more information, see System Status and Management, page 24.

7.6 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 12:55:42 PM	Hello, Telex! Log off
	About CMS
	Console Management System (CMS)
	Version: 0.8.4.38
	Bosch Security Systems, LLC
	130 Perinton Parkway
System —	Fairport, NY 14450
Status/Manage	USA
Network	(800)-752-7560
Settings	www.telex.com/radiodispatch
Log Settings	
SSL Settings	End-User License Agreement
Licensing	
About CMS	
	© Copyright 2022 Bosch Security Systems, LLC. All Rights Reserved. Version: 0.8.4.38
8 Design Manager Configuration and Operation 8.1 User/Role Creation

1 User/Role Creation

Design management utilizes the same username and password as the CMS web software. For more information, see *Account Management*, page 17.

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.

8.2 CMS Design Repository

8.2.1 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.

File name:	Default.veg ~
Save as type:	C-Soft Designer Files (*.veg) 🗸 🗸
	C-Soft Designer Files (*.veg)
	Telex Design Archive (*.tda)
 Hide Folders 	All Files (*.*)

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

8.2.2 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**.
- Click the Upload File button at the bottom of the screen. The Design Manager - Upload File screen opens.

TELEX 3:47:29 PM			Hello, Telex!	Log off
Contacts + CryptoSync +	Design Mar	nager - Upload File		
I/O Gateway +	Upload:	Browse) No file selected.		
Design Manager	Design Name			
Files Users	Enable Time Span	Start lime 12:00 AM © End lime 11:59 PM © Check All Sunday OMonday Tuesday Wednesday Thursday Priday Saturd	lay	
Accounts + System +	Assigned Roles			
	Administrator × Dis	patcher ×		
	telex × Telex_user			
	Back Upload	© Copyright 2022 Bosch Security Systems, LLC. All Rights Re	served. Version:	: 0.8.4.38

- 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**

8.2.3 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.

Design Manager - Files									
Search:									
File Name 🏦 Design Nam	e îl Date Uploaded	1 Start Time 1	End Time 斗	Days Active					
O CSSI Demo 2_7752.tda CSSI Demo	2_7752 1/12/2022	12:00 AM	12:00 AM	All					
Desktop CMS Demo.tda Desktop CM	S Demo 1/5/2022	12:00 AM	12:00 AM	All					
ECOM FEB 2022.tda ECOM FEB 2022.tda	022 2/9/2022	12:00 AM	12:00 AM	All					
GEORGIA DOT cms demo 2-22.tda GEORGIA D	DT cms demo 2-22 2/6/2022	12:00 AM	12:00 AM	All					
IP3008-v7752.tda IP3008-v77	2/2/2022	12:00 AM	12:00 AM	All					
NexEdge Gen 2 _7752 Laptop.tda NexEdge Gen	n 2 _7752 Laptop 1/26/2022	12:00 AM	12:00 AM	All					
SHHI Laptop Demo 7.752.tda SavannahA	rport Demo with SIP 2/9/2022	12:00 AM	12:00 AM	All					
© SIP_7752.tda SIP_7752	1/12/2022	12:00 AM	12:00 AM	All					
• tablet_demo_2-22.tda tablet_dem	2/6/2022	12:00 AM	12:00 AM	All					
UTE Mountain Position 1 7.752.tda UTE Mountain	in Position 1 7.752 1/19/2022	12:00 AM	12:00 AM	All					

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.

TELEX 12:31:23 PM			Hell	o, Telex! Log off
Contacts +	Design N	1anager - Edit File		
CryptoSync + I/O Gateway +				
Packet Forwarding	File Name	Desktop CMS Demo.tda		
Design Manager —	Replace File:	Browse No file selected.		
Files	Design Name	Desktop CMS Demo]	
Users	Enable Time			
System +	Span			
	Enable Days of Week			
	Assigned Roles			
	- Administrator	•		
	Assigned Users			
	✓ Telex_user ×			
	Back	Save © Copyright 2022	Bosch Security Systems, LLC. All Rights Reserve	d. Version: 0.8.4.38
4. Click the	Delete icon to	o remove the design fro	m the design repository.	

Bosch Security Systems, LLC

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

8.3 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 8.1: 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 8.2: 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.

8.3.1 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.

8.4 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.



- 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**.
- 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.

8.5 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.

	TELEX	×
	Sign in to C-Soft	
User I Q	Name	
Passw	vord	
ø	Login	(B)

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 17*.
- 2. Press the **Login button**.

If only one design is assigned to the user (or user's role) in *CMS Design Repository, page* 37, 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.

Sele	ct a Design	×
		Browse
-	Alpha_Romero 12/16/2021 1:45:20 PM -05:0	0
٩.	Alpha_Tauri 12/16/2021 1:45:51 PM -06:0	0
5	Alpine 12/16/2021 1:46:14 PM -06:0	0
۳.,	Aston_Martin 12/16/2021 1:46:32 PM -06:0	0
	Ferrari 12/16/2021 1:46:47 PM -06:0	o
•	Haas 12/16/2021 1:47:00 PM -06:0	o 🦂
	Launch	

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**.

9 Contact Management and Operation

9.1 Dispatch Position Setup

9.1.1 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.

i

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.

9.1.2

CMS Alias Updates for the Design

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

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

E	xternal Systems Setup	\times
	Console Management System API Setup The Console Management System hostname/IP address and port settings are configured using either Console Configuration Tool or Telex System Manager.	
	Contact Management CryptoSync Enable Alias Updates from CMS Authorization Token xm7qOEnjIxscimwK	
	OK Cance	1

3. Select the Enable Alias Updates from CMS check box.

4. Click **OK**.

9.2 Contact Overview

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

Users

The **User Contacts table** 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.

User	Contacts					;	Table Version:
) 1.	Alias	I	ID		m	Tx Inhibit	
de:	Alias	xxxxxxxxxxx		Generic	*	× A	dd
Search:							
	Alias 🏦	ID 11	System	11	Tx I	nhibit	
	Alex	2541	P25-CSSI			×	Ø
	CSSI_TEST_4	4	Generic			×	ľ
	GWash	1234	MDC-1200 Generic		~	Ø	
	Test	123				×	Ø
	Test 2	321	Generic			×	Ø
	Test 3	333	Generic			×	C
	Test 4	5	Generic			×	Ø
Show	10 🕈 entries					Showing	1 to 7 of 7 ent

Figure 9.1: 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.

TELEX 12:44:43 PM							He	lo, Telex! Log off		
Contacts – Users Groups	Group	Contact	S				Ta	able Version: 3		
SIP Contacts SIP Directories						тх				
CryptoSync +		Group		ID	System	Inhibit	Color			
1/O Gateway 🕂		Alias	xxxxxx	xxxx	Generic		Ado			
Packet Forwarding	Coardhu									
Design Manager	Search.									
+	Alias	1. 1	D 11	System	n †l	TX Inhibit	Colo	r		
System +	NASA		457815		ric	~		Ø		
	Show 10 + entries									
				First Previou	ıs 1 Next	Last	Showing 1	.0 1 0/ 1 endles		
		-								
	Import CSV	Export CSV	Import S	System List	Delete All	s	ave			

Figure 9.2: 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.

ories	First Name	Last Name	Display Name	Number	Subdirectory	
+	John	Doe	John Doe	200000000000	Global Direct 🗸	Add
i +	2.000 kg					
arding	Search:					
ger +	First Name 🏦	Last Name	Display Name	11	Number 👘	Sub Directory
#	Jane	Star	JStar		4568	Global
+	John	Public	JPub		1234	Global Directory
	John	Public	JPub		1234	Global Directory
	Show 10 ¢ entries				Sh	owing 1 to 3 of
		Fir	st Previous 1 N	ext Last		

Figure 9.3: 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.

TELEX 1:54:03 PM					Hello, Telex! Log off					
Contacts – Users Groups	SIP Dir	ectories			Table Version: 1					
SIP Contacts			Name							
CryptoSync +		Sub Directory		Add						
	Search:									
			Name							
			Global Directory							
			Ø							
	Subdirectory 2									
			Subdirectory 3							
			Subdirectory 4		Ø					
			Subdirectory 5							
			Subdirectory 6		Ø					
	Show 10	 entries 	First Previous 1 Next L	Showir	ng 1 to 7 of 7 entries					
	Save		© Copyright 2022 Bosch Securi	ity Systems, LLC. All Rights Re	served. Version: 0.8.4.38					

Figure 9.4: 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.

9.2.1 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.

9.2.2 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.



9.2.3 Export CSV

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



Fi	ile Ho	me Inse	rt Pa	age L For	mu I	Data	Review	Vie	ew Help	A	croba	ß	P	
Clip	board v	Font	Aligni ~	ment Ni	% umber ~		Condit Format Cell Sty	iona : as T /les ` Sty	l Formatt Table ~ Y Yles	ing ~	Cell	s	Ec >	~
AutoSave 💽 🚰 🦻 Y 🖓 👻 🤿														
A1		• :	×	 ✓ 	f_{x}	Uni	t Name							~
	Α	В		С	[)	E		F		G		н	
1	Unit Nar	ne <mark>l</mark> Unit ID) T	TX Inhibit	Туре		Filters		lcon					П
2	CSSI_TE	S	4	0	Gene	ric	None			0				
3	Alex	2	541	0	P25-	CSSI	None			0				
4	Test		123	0	Gene	ric	None			0				
5	Test 2		321	0	Gene	ric	None			0				
6	Test 3		333	0	Gene	ric	None			0				
7	Test 4		5	0	Gene	ric	None			0				
8	GWash	1	234	1	MDC	-1200	None			0				
9														
10														
11														
12			- L.											•
	∢ →	Use	ers	Ð				:	•				Þ	
Rea	dy						E	巴			-	- +	100%	5

9.2.4 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.



9.2.5 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.

10 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



10.1Broker Settings Page

TELEX 12:50:19 PM			Hello, Telex! Log off
Contacts + CryptoSync +	Broker Settings		
I/O Gateway —	MQTT Broker Connection		
Broker Settings Device Settings	Broker IP	127.0.0.1	
Packet Forwarding	Broker Port	1883	
Design Manager +	User Name		
Accounts +	Password	Change Password	
System +	Enable TLS Connection	0	
	Console Multicast Settings		
	Console Multicast Address	225.8.11.81	
	Console Multicast Port	2026	
	Console Multicast TTL	6	
	Save	© Copyright 2022 Bosch Security Systems, LLC. All Rig	hts Reserved. Version: 0.8.4.38

Figure 10.1: 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.

10.2 Device Settings Page

TELEX 3:43:17 PM						Hello, Telex!	Log off
Contacts + CryptoSync +	Device Setting	S					
I/O Gateway —	NOTE: Chang	ges to this data tab	ole are saved IMMED	IATELY. The upload button se	ends the current table to th	he service.	
Broker Settings		A	lias	MAC Address			
Packet Forwarding		Alias		00:00:00:00:00:00	Add		
Design Manager +							
Accounts +	Device Alias	ţ1 I	MAC Address		11		
System +	TestAdam	(00:D0:C9:EF:D8:7F		ß	â	
	TestAdam2		00:D0:C9:EF:D8:7f			â	
	Upload to Service			© Copyright 2022 Bosch Sec	curity Systems, LLC. All Rig	hts Reserved. Version	: 0.8.4.38

Figure 10.2: 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 $\ensuremath{\textbf{MAC}}$ $\ensuremath{\textbf{Address}}$ 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.

10.3 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

10.3.1 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-60 50	Terminal DO 0 and Iso GND are used for Relay #1, terminals DO 1 and Iso GND are used for Relay #2, etc.
ADAM-60 60	Terminals RL 0+ and RL 0- are used for Relay #1, terminals RL 1+ and RL 1- are used for Relay #2, etc.
ADAM-62 66	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.

10.4 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.

10.4.1 Configure the Mosquitto Broker

1	-	

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.

 Using a terminal text editor, edit the following file with sudo: /usr/lib/system/ mosquitto.service.

Use the root password set in configuration.

- 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.

10.4.2Enable TLS in CMS

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

Contacts +			
CryptoSync +	Broker Settings		
I/O Gateway – Broker Settings Device Settings Packet Forwarding Design Manager + Accounts + System +	MQTT Broker Connection Broker IP Broker Port User Name Password Enable TLS Connection	127.0.0.1 1883 Change Password	
	Console Multicast Settings Console Multicast Address Console Multicast Port Console Multicast TTL	225.8.11.81 2026 © 6 ©	

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

10.5 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.

10.5.1	Mosquito Broker Configuration
(i)	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.
í	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.
	 SSH into the CMS unit with an SSH client as the telex user and the password set during configuration. Create a file in /etc/mosquitto/ called password with sudo. Using a terminal text editor, edit the password file you just created with sudo. 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. Save and close the file. Run the command: sudo mosquitto_passwd -U /etc/mosquitto/password. Using a terminal text editor, edit the following file with sudo: /usr/lib/systemd/ system/mosquitto.service. Use the root password set in configuration. 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
	 Save the file. Save the command: sudo systemctl daemon-reload. Run the command: sudo systemctl restart mosquitto.service. Mosquitto is now configured to use tls/ssl and user authentication

10.5.2 Console Management System Configuration

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

9:37:44 AM			Hello, Telex! Log off
Contacts + CryptoSync +	Broker Settings		
I/O Gateway —	MQTT Broker Connection		
Broker Settings Device Settings	Broker IP	127.0.0.1	
Packet Forwarding	Broker Port	1883 0	
Design Manager +	User Name	Bob	
Accounts +	Password	•••••••••• Change Password	
System +	Enable TLS Connection		
	Console Multicast Settings		
	Console Multicast Address	225.8.11.81	
	Console Multicast Port	2026	
	Console Multicast TTL	6	
	Save	© Copyright 2022 Bosch Security Systems, LLC. All Rights Re	served. Version: 0.8.4.38

- 2. Enter a **user name**.
- 3. Click the **Change Password button**. The Change Password screen appears.

Change Password

New Password

Save changes

Close

х

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

10.5.3 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.

6 H 0 M 7 B >	m 55 (i)				
Cont Cont Cont Cont Cont Cont Cont Cont	Information Network S MGTT SNTP Assee	team/Trap Administration Firmware P2PEr	ent Access Control	Modbus Address C	bud
Burnet	Publish / Subscribe	Enable DeviceOn/BI MOTT	Enable		Anoly .
10 0 0 15 (ADAM-6080)	Host	172 19 100 135 8883	43	(Only Inc	Aude Basic Settings)
Others	TLS:	🖸 Enable			
ADAMAS00_5510Sense	User Name :	***	Password :		
O music see assort	Heartbeat	5 second(x)	Deathanit	100	mill-second(s)
	Retain Message	Enable			
	Basic Settings Adve	noed Settings			
	WII Tepic :	Advantech/74FE485EFEAD/Device_8	Mur		
	Publish GoS	0 ~			
	Publish Topic	Enable Publish Topic		Channel Type	
		Laurench/215E135E2E2	(Maha	di i	

- 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.

11

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.



11.1 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.

2:03:34 PM						Hello	o, Telex! Log off
	Packet For	wardin	g				
I/O Gateway +	Rules						
Design Manager	Rule Name 📫	Enabled	Source Address	Source Port	Destinations	Activity	
	Pulo 1		225.0.11.01	1054			
	Rule I	Ŷ	225.0.11.01	1054	I	•	C D
	Rule 2	~	225.8.11.81	1056	4	•	æ
	Showing 1 to 2 of 2	entries				Previou	s 1 Next
	Add Rule Copy Ru	ule Dele	te All Rules				

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

TELEX 3:36:25 PM					Hello, Telex! Log off
Contacts + CryptoSync +	Edit Rule				
I/O Gateway + Packet Forwarding	Source Settings				
- Design Manager	Rule Name ↑↓	Enabled	Source Address	Source Port	Actions
+ Accounts +	Rule 1	*	225.8.11.81	1054	ß
System +	Destination Settings				
	Destination Name	†↓ Enabled	Destination Address	Destination Port	TTL Actions
	Destination 1	~	225.8.11.81	3054	6
	Showing 1 to 1 of 1 entries				Previous 1 Next
	Cancel Add Destination	Add Range Dele	ete All Destinations	e	

3. Click the edit icon next to the rule you want to modify.

The Source Setting screen opens.

Rule 2	×
Rule Name Rule 2	Is Enabled 🗹
Source IP Address	Source Port
225.8.11.81	1056
	Save Cancel
 Make the desired changes. Click the Save button. The Source Setting screen closes. 	
Notice! The default rule is disabled by default. and allow UDP packets to rebroadcast.	Select the Is Enabled checkbox to enable the Rule

To edit the Destination settings, do the following:

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

Destination Name	Is Enal	oled 🔽
Destination 3		
Destination IP Address	Destination Port	
225.8.11.81	1054	
TTL		
6		

- 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.
- 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.

12:53:49 PM		Add Destin	ation Rang	je	×	Hello,	Telex! Log off
ontacts + rvptoSvnc +	Edit Rul	Name Increment By	Destir	nation			
O Gateway 🕂		IP	225.8	Number 3.11.81			
acket Forwarding	Source Settir	Port	1054				
esign Manager +	Rule Na	Count	2		Source	ce Port	Actions
counts +	Rule	TTL .	6		10	054	œ
ystem +	Destination S			Add Ca	incel		
	Destination	Name †↓	Enabled	Destination Address	Destination	Port TTL	Actions
	Destinal	tion 1	*	225.8.11.81	3054	6	C î
	Destinal	tion 2	*	225.8.11.81	1073	6	C û
	Showing 1 to 2	of 2 entries				Previo	us 1 Next
	Cancel Add [Destination	Add Rang	e Delete All Destinati	ons	Save	

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

11.2 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.

2:03:34 PM						Hell	o, Telex! Log off
	Packet For	wardin	g				
	· · · · · · · · · · · · · · · · · · ·						
I/O Gateway +	Rules						
Design Manager	Rule Name 1	Enabled	Source Address	Source Port	Destinations	Activity	
	Bula 1		225.0.11.01	1054			
	Kule I	Ŷ	225.0.11.01	1054	I	•	
	Rule 2	~	225.8.11.81	1056	4	•	6
	Showing 1 to 2 of 2	entries				Previou	is 1 Next
	Add Rule Copy Ru	Je Dele	te All Rules				

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

TELEX 3:36:25 PM					Hello, Telex! Log off
Contacts + CryptoSync +	Edit Rule				
Packet Forwarding	Source Settings				
Design Manager	Rule Name	Enabled	Source Address	Source Port	Actions
+ Accounts +	Rule 1	~	225.8.11.81	1054	ß
System +	Destination Settings				
	Destination Name	†↓ Enabled	Destination Address	Destination Port	TTL Actions
	Destination 1	*	225.8.11.81	3054	6
	Showing 1 to 1 of 1 entries				Previous 1 Next
	Cancel Add Destination	Add Range Dele	ete All Destinations Save		

3. Click the edit icon next to the rule you want to modify.

The Source Setting screen opens.

Rule 2		×
Rule Name		Is Enabled 🗹
Rule 2		
Source IP Address	Source Port	
225.8.11.81	1056	
	Save	Cancel
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.

11.3 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.



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



Technical Manual

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

3:03:22 PM							Hello, Telex! Lo
Contacts + CryptoSync +	Edit Rule						
Packet Forwarding	Source Settings						
Design Manager	Rule Name ↑↓	Enabled	Source Address		Source Po	rt	Actions
+ Accounts +	Rule 2 Copy	*	225.8.11.81		1057		Ø
System +	Destination Settings						
	Destination Name 斗	Enabled	Destination Address	Des	tination Port	ΠL	Actions
	Destination 1	*	225.8.11.81		1075	6	C D
	Destination 2	*	225.8.11.81		1074	6	2
	Destination 3	*	225.8.11.81		1055	6	C D
	Destination 4	*	225.8.11.81		1056	6	C D
	Showing 1 to 4 of 4 entries					Pre	vious 1 Next
Ca	ncel Add Destination	Add Range	Delete All Destinations		Save		

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

8:00 PM	R	ile 2 Copy		×		
istis + 2.Sync +	Edit Rule	le Name Rule 5	Is Er	nabled 🗹		
iteway +	So	urce IP Address	Source Port			
: Forwarding	Source Settings	25.8.11.81	1057	_		
n Manager	Rule Name		Save	Cancel Source P	ort	Actions
nts +	Rule 2 Copy			1057		œ
n 4.	Destination Settings					
	Destination Name	1 Enabled	Destination Address	Destination Port	TTL	Actions
	Destination 1	~	225.8.11.81	1075	6	C i
	Destination 2	~	225.8.11.81	1074	6	C i
	Destination 3	~	225.8.11.81	1055	6	6 9
	Destination 4	~	225.8.11.81	1056	6	C Ó
	Showing 1 to 4 of 4 entri	es			Prev	ious 1 Nex

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

11.4 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.

Contacts +						Hello	, Telex! Log of
	Packet For	wardin	g				
CryptoSync +							
I/O Gateway +	Rules						
Packet Forwarding	Rule Name 📫	Enabled	Source Address	Source Port	Destinations	Activity	
+	Dula 1	Lindbied	225.0.11.01	1054	-	, icervity	
Accounts +	Rule I	•	225.8.11.81	1054	I	•	۵ (D
System +	Rule 2	~	225.8.11.81	1056	4	•	7
	Showing 1 to 2 of 2 of	entries				Previous	1 Next
1							

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

2:36:53 PM		D	elete Rule	×	c		
Contacts +	Packet Forwa	rding ^	re you sure you wish to delete th	nis rule?			
CryptoSync +				Delete Cancel			
Packet Forwarding	Rules						
Design Manager	Rule Name 🏦	Enabled	Source Address	Source Port	Destinations	Activity	
+ Accounts +	Rule 1	*	225.8.11.81	1054	1	۲	C D
System +	Rule 2	~	225.8.11.81	1056	4	۲	C i
	Add Rule Copy Rule	S Delete All Rt	иes	© Copyright 20	22 Bosch Security System	ns, LLC. All Rights	Reserved. Version: 0.8.4.38

3. Click **Delete**.
12CryptoSync Configuration and Operation12.1CryptoSync 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.

TELEX 12:35:36 PM			Hello, Telex! Log off
Contacts + CryptoSync -	CryptoSync Setti	ngs	
Status Settings I/O Gateway + Packet Forwarding Design Manager + Accounts + System +	Key Refresh Period (s) Authorization Token	3600 ae1798590f5d68bb	
	Save	© Copyright 2022 Bosch Security Systems, LLC. All Rights R	eserved. Version: 0.8.4.38

Figure 12.1: 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.

12.2 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**.

CMS SETUP

IP Address:	172.19.30.30
Control Port:	7554
SRTP Encryption:	
Authorization Token:	0qGVRN7vHwPK2CRq

- 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.

12.3 C-Soft Configuration

12.3.1 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.

12.3.2 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.

External Systems Setup		\times
Console Management System API	Setup	
The Console Management System using either Console Configuration	hostname/IP address and port settings are configured Tool or Telex System Manager.	
Contact Management	CryptoSync	
Enable Alias Updates from Cl	MS Authorization Token	
	xm7qOEnjIxscimwK	
	OK Cancel	

- 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.

Line Options Setup: Line 1	×
Line Setup Options Vocoder Type TELEX 32K ~	OK Cancel
TX Monitor Enable Scannable	
Packet Delay for Satellite Mode	
Backup IP Setup Multicast Address Port	
RX: 0.0.0.0 1054	
TX: 0.0.0.0 1254	
Base Radio IP: 0 . 0 . 0 . 0	
Encryption Setup	
SRTP Encryption	

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

12.4 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.

TELEX 3:32:37 PM

Source Device 1	Device Type	Source IP	Line Name 📫	Endpoint 11	SSRC 11	Listeners 斗	Statu
Dispatch Position A	C-Soft	172.20.100.3	Line 1 SRTP	225.8.11.85:1080	40538	Dispatch Position B	Acti
Dispatch Position A	C-Soft	172.20.100.3	Line 2 SRTP	225.8.11.85:1081	41813	Dispatch Position B	Acti
Dispatch Position A	C-Soft	172.20.100.3	Line 3 SRTP	225.8.11.85:1082	53445	Dispatch Position B	Acti
Dispatch Position A	C-Soft	172.20.100.3	Line 4 SRTP	225.8.11.85:1083	51569	Dispatch Position B	Activ
Dispatch Position B	C-Soft	172.20.100.1	Line 1 SRTP	225.8.11.85:1080	36222	Dispatch Position A	Activ
Dispatch Position B	C-Soft	172.20.100.1	Line 2 SRTP	225.8.11.85:1081	31490	Dispatch Position A	Activ
Dispatch Position B	C-Soft	172.20.100.1	Line 3 SRTP	225.8.11.85:1082	34718	Dispatch Position A	Acti
Dispatch Position B	C-Soft	172.20.100.1	Line 4 SRTP	225.8.11.85:1083	22984	Dispatch Position A	Acti

Figure 12.2: 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.

3:32:33 PM Contacts +	CryptoSync Status				
CryptoSync – Status Settings I/O Gateway +	Endpoint List				
Packet Forwarding	Source Device 1	Device Type	Source IP	Line Name 11	Endpoint 1
Design Manager 🕂	Dispatch Position A	C-Soft	172.20.100.3	Line 1 SRTP	225.8.11.85:1080
Accounts +	Dispatch Position A	C-Soft	172.20.100.3	Line 2 SRTP	225.8.11.85:1081
System +	Dispatch Position A	C-Soft	172.20.100.3	Line 3 SRTP	225.8.11.85:1082
	Dispatch Position A	C-Soft	172.20.100.3	Line 4 SRTP	225.8.11.85:1083
	Dispatch Position B	C-Soft	172.20.100.1	Line 1 SRTP	225.8.11.85:1080
	Dispatch Position B	C-Soft	172.20.100.1	Line 2 SRTP	225.8.11.85:1081
	Dispatch Position B	C-Soft	172.20.100.1	Line 3 SRTP	225.8.11.85:1082
	Dispatch Position B	C-Soft	172.20.100.1	Line 4 SRTP	225.8.11.85:1083
	Show 10 • entries		Previous Next		Showing 1 to 8 of 8 entries
			60	Copyright 2022 Bosch Security Systems	LLC. All Rights Reserved. Version: 0.8.4.3

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 Frequently Asked Questions

CMS Configuration

Question	Answer		
What if the wrong IP	Connect a monitor and keyboard to the units. Run the script		
information for the	factoryreset.sh found in /home/telex/utilities to rest the		
cluster is entered in the	devices back to factory settings.		
CMS Configuration?	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 <i>Log Settings, page 28</i> page.
Can I use my own SSL certificate?	Yes. Upload your SSL certificate under SSL Certificate, page 29.
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 <i>System Status and Management, page 24</i> 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 24. 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 <i>System Status and Management, page 24</i> . 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.

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.

Contact Management

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	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.
adapters?	

Design Manager

Question	Answer
How can I easily view what designs users are assigned?	You can view overall user design assignments from the <i>Design</i> Manager Configuration and Operation, page 37 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	No, due to limitations with windows remote desktop
Launcher over a	connection, Console Launcher cannot be used. C-Soft can still
window's remote	be used by accessing csoftruntime.exe in C:\Program Files
desktop connection?	(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 <i>System Status and</i> <i>Management, page 24</i> and your current connections licenses in
	Licensing, page 33.

14 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.

Energy Star is a registered trademark of U.S. Environmental Protection Agency, all rights reserved.

Hewlett Packard and the HP logo are registered trademarks of Hewlett Packard, all rights reserved. All data and dimensions are referenced from the Hewlett Packard QuickSpecs and are subject to change without notice.

Intel is a registered trademark of Intel; Xeon, Core and vPro are trademarks of Intel, all rights reserved.



Bosch Security Systems, LLC 130 Perinton Parkway

Fairport, NY 14450 USA www.telex.com © Bosch Security Systems, LLC, 2024

EU importer: Bosch Sicherheitssysteme GmbH Robert-Bosch-Platz 1 70839 Gerlingen Germany © Bosch Sicherheitssysteme GmbH, 2024