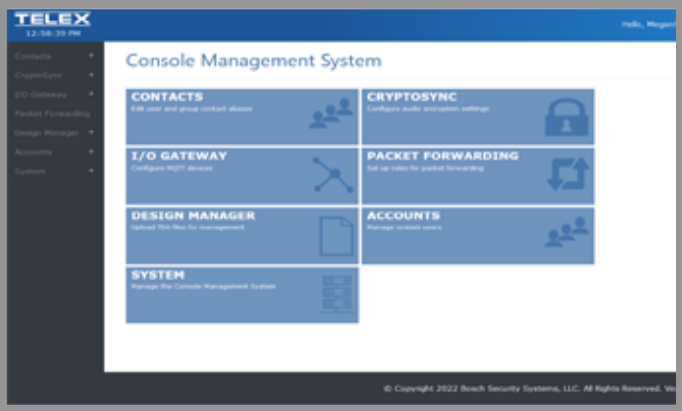
TELEX

Console Management System



en Quick Install Guide

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@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.

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 Quick Installation

Required Equipment

– Console Management System Workstation

Workstation Setup and Configuration

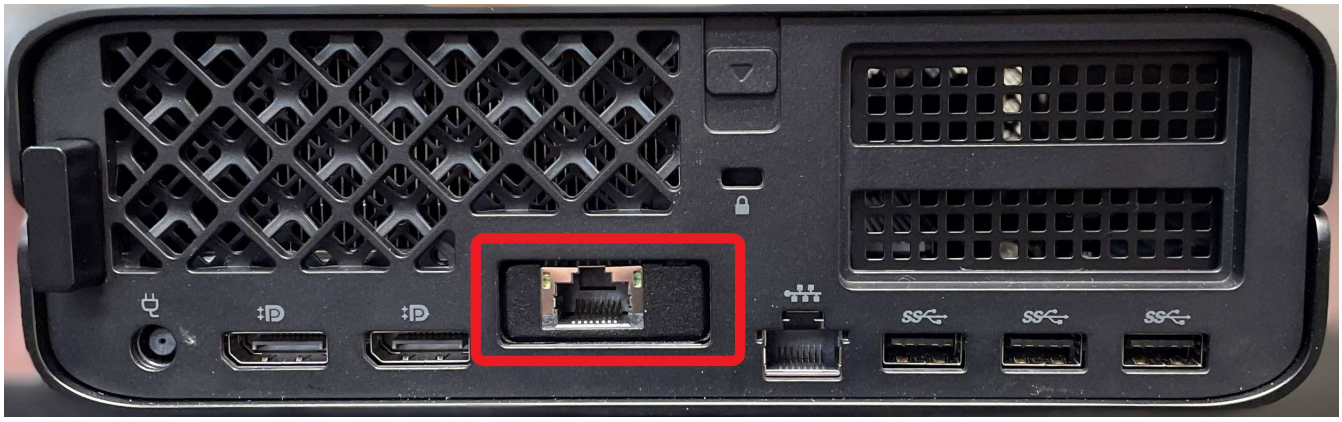
Box Contents

– 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.

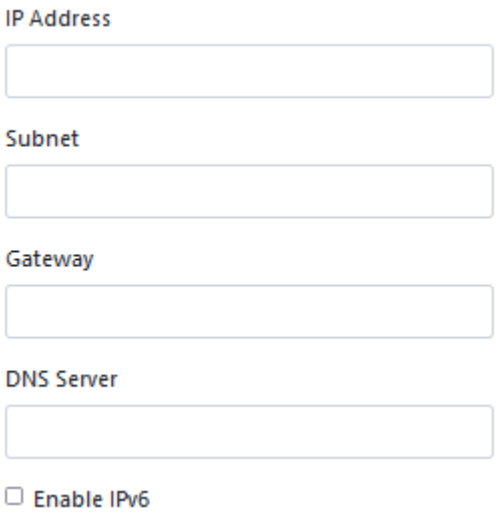
4. Enter the **Linux Root password** you want to use.
5. Enter the **Linux User password** you want to use.
   The default Linux username is **telex**.

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.

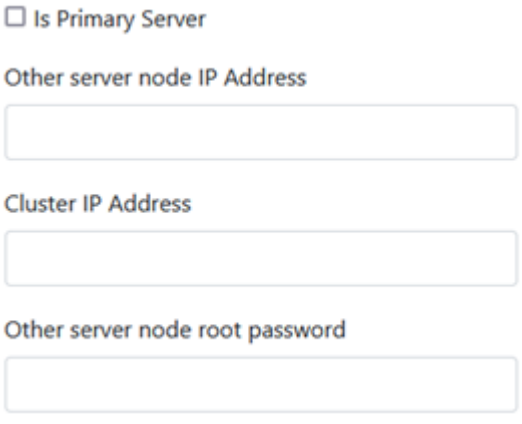


Notice!
You can also set the IPv6 configuration, but it is not required.

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

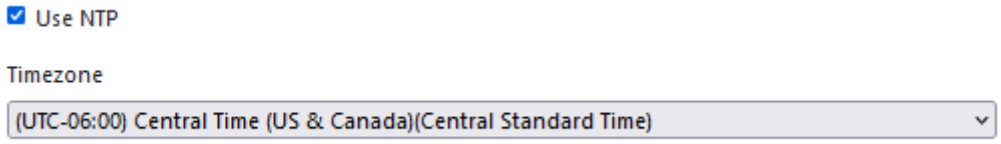
Notice!
Set only one server as the primary server. If both are set, the cluster configuration will fail.

   - **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.



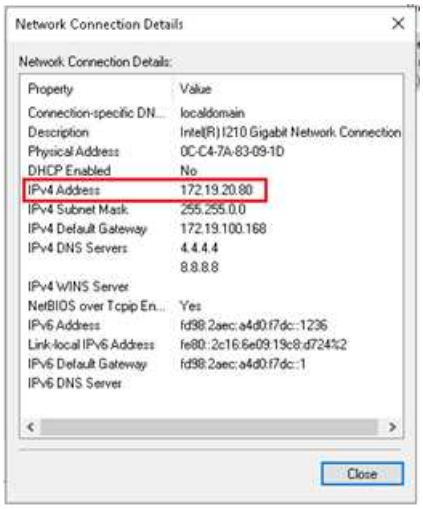
Notice!
By default, NTP is enabled on the device and the date time field are not shown. If you choose to set your own date and time, clear the NTP check box and set those fields.

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. Please refer to the License Installation Instructions (P/N F.01U.406.722) for further information.

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

202403181804