

## PRESENTATION

### Référence produit : 595.0000 (XE2 MED TOUCH)

Votre équipement d'interphonie SIP propose les fonctionnalités suivantes :

- Etablir une communication audio avec des postes de la gamme interphonie sur IP Castel, des Softphones, ou tout autre équipement compatible avec la norme SIP :
  - ↳ En point à point
  - ↳ En s'enregistrant sur un serveur SIP avec la possibilité de configurer jusqu'à 2 serveurs de secours et du multi compte SIP
- Etablir une communication audio avec les postes d'interphonie de la gamme numérique et analogique Castel (nécessite l'utilisation d'une passerelle supplémentaire M-HYB-IP)
- Embarque un serveur Web permettant la configuration et l'exploitation depuis n'importe quel navigateur
- Embarque des mécanismes de cybersécurité, notamment :
  - ↳ Firewall avec listing des services et ports actifs
  - ↳ Politique de sécurité appliquée aux utilisateurs et aux services externes
  - ↳ Restriction par plage IP
  - ↳ Sécurisation des connexions Ethernet via le protocole 802.1X (RADIUS)
- Gestion de profils, sélectionnables par plage horaire ou via des automatismes
- Gestion d'automatismes évolués (relations logiques et horaires) sur ses interfaces
- Support des services suivants :
  - ↳ SNMP (Simple Network Management Protocol)
  - ↳ Notification vers des superviseurs via des chaînes ASCII
- Interfaçage natif avec la solution de contrôle d'accès Synchronic
- Autotests pouvant être exécutés automatiquement ou à la demande
- Support des langues suivantes : Français / Anglais / Espagnol / Polonais / Néerlandais



Il dispose des caractéristiques suivantes :

- Ecran tactile de 7 pouces
- 2 entrées "Tout ou Rien"
- 2 contacts secs pour commander une gâche ou tout autre équipement
- Alimentation externe, PoE (Power Over Ethernet) ou PoE+ (Power Over Ethernet Plus)
- 2 ports Ethernet 10/100/1000MB permettant 1 connexion bridge (permet la connexion d'un autre système IP) + support des VLAN.

## RACCORDEMENT

FR

EN

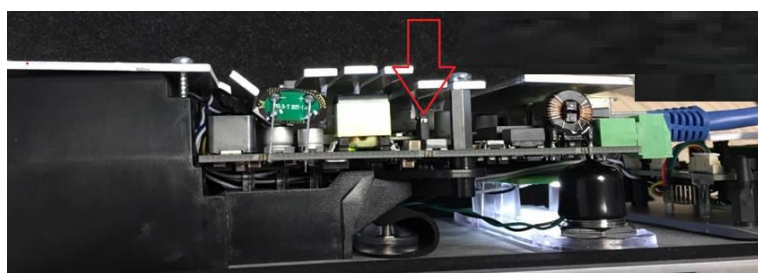
### Raccordement de l'alimentation (24VDC)

L'alimentation requise est de 20 à 30VDC.

Remarque : le portier peut être alimenté par le réseau Ethernet en PoE+ ou PoE (avec certaines restrictions)

Votre portier est livré d'usine en configuration PoE/PoE+, toutefois dans certains cas il peut être nécessaire de le bloquer dans une configuration PoE seul (répartition de la puissance du Switch sur plusieurs portiers/ mauvaise gestion de l'alimentation du Switch/ ...).

Dans ce cas avec le portier non alimenté et avec une petite pince non conductrice, retirer le strap indiqué en rouge sur la photo ci-dessous



### Raccordement au réseau IP (ETH0 / ETH1)

Le raccordement se fait par une liaison Ethernet 10/100/1000 Mbits RJ45 classe 5e ou 6.

2 Ports Ethernet sont disponibles (1 compatible PoE ou PoE+ et 1 non PoE)

### Raccordement de la sortie 0dB (0dB +/-) Applicable à partir de la version software 1.5.0

Une sortie **différentielle** 0dB permet le raccordement d'un ampli externe.

+ : Point chaud

- : Point froid

0V : Masse

### Raccordement au bus RS485 VDIP (RS1 / RS2 / 0V) Configurable par CASTELSuite

Le portier permet de gérer jusqu'à 4 périphériques VDIP (VD4S réf 110.1000, VD8EI réf 110.1100, VDLECT réf 110.1200) via une ligne bus RS485 (câblage en bus : plusieurs périphériques sont installés sur une même ligne bus).

La liaison bus entre les périphériques et le portier est réalisée par les points RS1, RS2 (via une paire torsadée) et la masse. Etablir la connexion point à point en respectant l'ordre des signaux.

La longueur maximale du bus est de 1Km. Il est nécessaire d'installer une résistance de 120Ω (fournie avec le périphérique) entre les points RS1 et RS2 à chaque extrémité du bus.

### Raccordement des entrées (IN1 / IN2 / 0V)

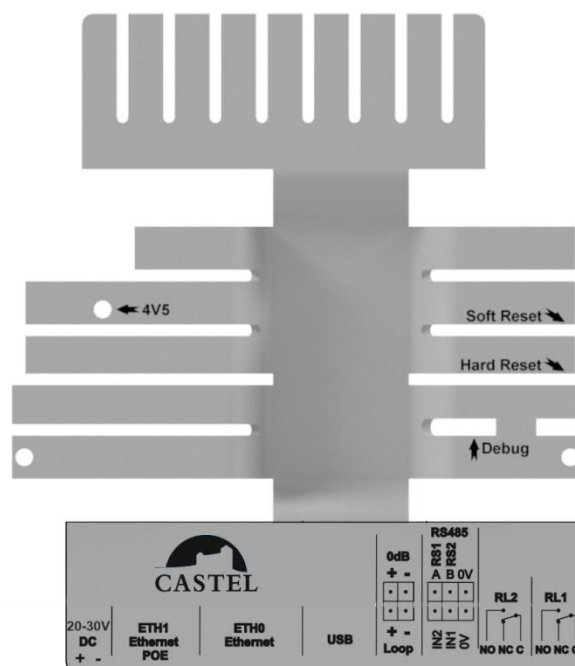
Deux entrées TOR permettent le raccordement d'un contact sec (ne pas appliquer de tension). Pour être activée, l'entrée doit être tirée à la masse.

Le contact peut être déporté jusqu'à 1Km.

### Raccordement des sorties relais (RL1 / RL2)

Le raccordement se fait via un bornier 3 points fournissant l'interface « Commun (C) / Repos (NC) / Travail (NO) ».

Si vous utilisez une de ces sorties relais pour commander une gâche en AC ou DC, câbler une diode 58V non polarisée en parallèle sur le contact sec entre C et NO ou C et NC selon utilisation (diode fournie).



## INSTALLATION

FR

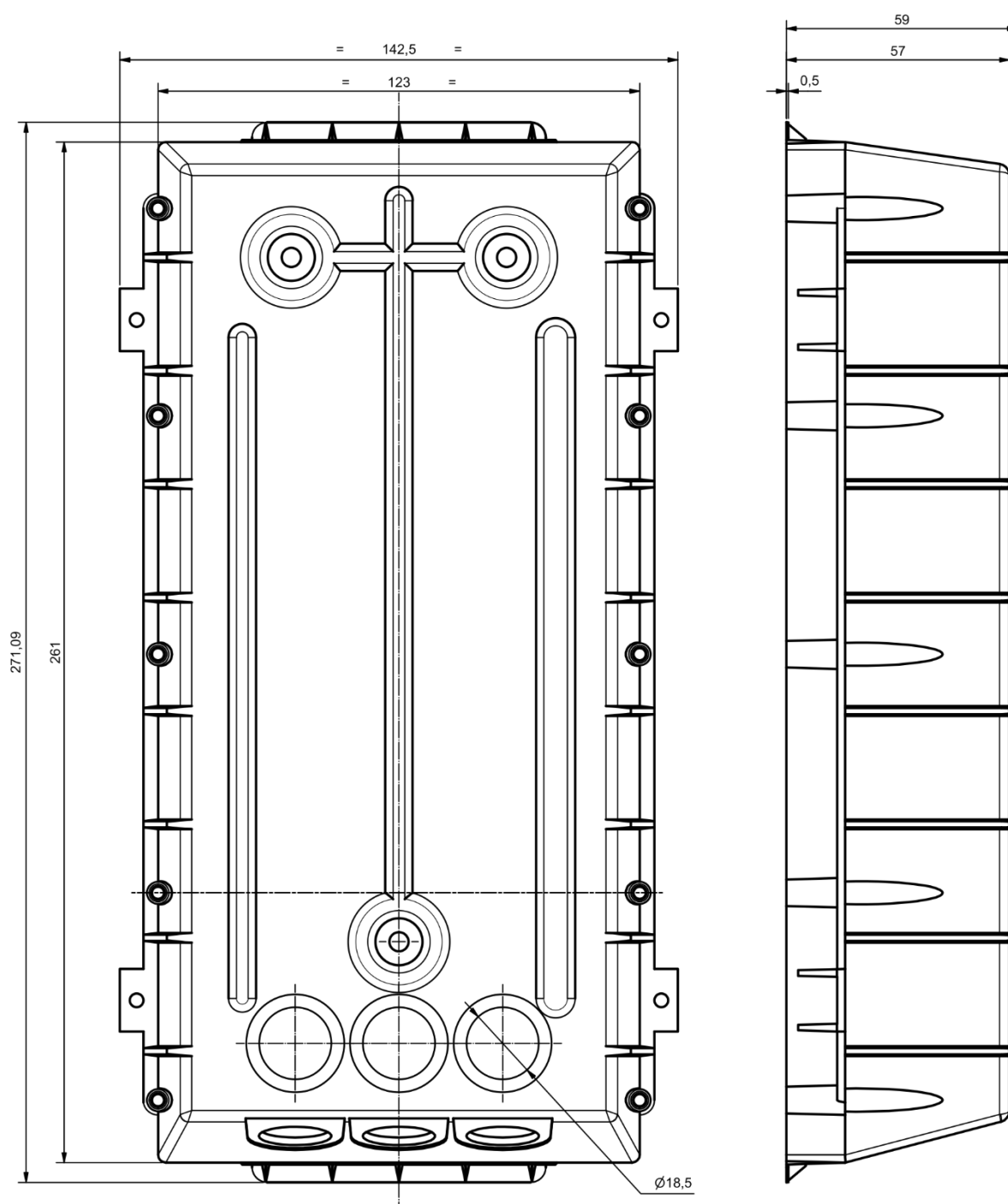
EN

### Montage en encastrement

- Faire une réservation dans le support d'une dimension minimum de hauteur 266mm, de largeur 145mm et de profondeur 64mm mini.
- Enduire le fond de la réservation d'au moins 10mm de ciment frais.
- Introduire le fond du portier dans la réservation et le pousser en appuyant les butées d'encastrement contre le support où a été faite la réservation.
- Laisser sécher le ciment au moins 24H, puis raccorder le portier.
- Positionner et clipser la platine sur le fond.

### Montage en encastrement sur placoplâtre

- Faire une réservation dans le support d'une dimension minimum de hauteur 266mm, de largeur 145mm.
- Pour le montage sur support BA13 (Placoplâtre), utiliser les griffes fournies, puis raccorder le portier.
- Positionner et clipser la platine sur le fond.



Cadre interface  
avec clipses

Fond

Face avant



Pour le démontage de la platine, utiliser un tournevis plat dont on introduira le bout dans la fente prévue à cet effet dans la partie inférieure de la platine puis effectuer une rotation de celui-ci et tirer manuellement afin de déclipser la platine de son support.

## UTILISATION

### Adresse IP du poste

Le poste est livré par défaut en DHCP. En cas d'absence de serveur DHCP, le poste récupère une adresse IP fixe du domaine IPV4LL : 169.254.xx.xx.

Il est possible de fixer l'adresse IP (IP statique) et les autres paramètres réseaux en modifiant la configuration du poste.

La découverte de l'adresse IP du poste est possible depuis :

- Le logiciel CastellIPSearch
- Le logiciel CastellServeur

Si la découverte de l'adresse IP du poste n'est pas possible :

- En configuration usine, le poste énonce son adresse IP lorsque l'on appuie sur le 1<sup>er</sup> bouton programmable
- Le poste énonce également son adresse IP lorsque l'on appuie brièvement sur le bouton poussoir « Soft Reset » présent sur la carte électronique
- Avec un appui maintenu supérieur à 3 secondes sur le bouton poussoir « Soft Reset », le poste fixe l'adresse IP à 192.168.49.251.

### Reset du poste

Un appui maintenu supérieur à 20 secondes sur le bouton poussoir « Soft Reset » entraîne un redémarrage du poste et la réinitialisation des paramètres en configuration usine.

Un appui sur le bouton « Hard Reset » entraîne uniquement le redémarrage du poste immédiatement.

### Accès au Serveur Web du poste

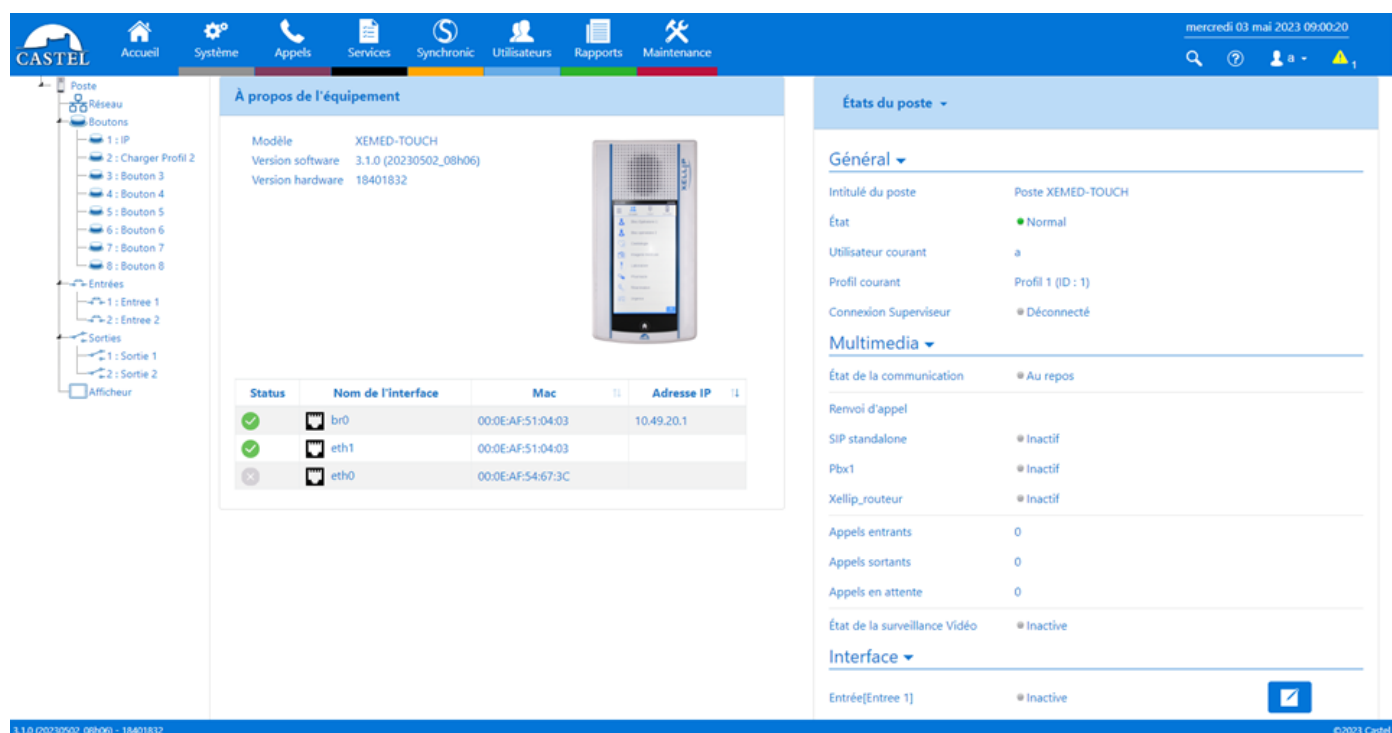
L'accès au serveur Web du poste est possible depuis un navigateur tel que Chrome, Edge ou Firefox.

Ouvrez votre navigateur à partir d'un équipement dans le même réseau et tapez : **https://[adresse\_ip\_du\_poste]**

Ensuite 2 situations sont possibles :

- Soit votre poste est en configuration usine, un wizard doit être renseigné avant toute autre opération
- Soit votre poste dispose déjà d'une configuration. Veuillez saisir le login et le mot de passe qui ont été définis par l'administrateur du site.

A noter : une aide en ligne est accessible à partir de tous les menus. Cette aide permet de s'informer sur les différentes fonctions du serveur Web.



The screenshot displays the Castell web interface for a XEMED-TOUCH device. The top navigation bar includes icons for Accueil, Système, Appels, Services, Synchronic, Utilisateurs, Rapports, and Maintenance. The main content area is divided into three sections:

- À propos de l'équipement:** Shows device details:
 

Modèle	XEMED-TOUCH
Version software	3.1.0 (20230502_08h06)
Version hardware	18401832

 Below this is a table of network interfaces:
 

Status	Nom de l'interface	Mac	Adresse IP
✓	br0	00:0E:AF:51:04:03	10.49.20.1
✓	eth1	00:0E:AF:51:04:03	
✗	eth0	00:0E:AF:54:67:3C	
- États du poste:** Shows general status:
  - Intitulé du poste: Poste XEMED-TOUCH
  - État: Normal
  - Utilisateur courant: a
  - Profil courant: Profil 1 (ID : 1)
  - Connexion Superviseur: Déconnecté
  - État de la communication: Au repos
  - Renvoi d'appel: Inactif
  - SIP standalone: Inactif
  - Pbx1: Inactif
  - Xellip\_routeur: Inactif
  - Appels entrants: 0
  - Appels sortants: 0
  - Appels en attente: 0
  - État de la surveillance Vidéo: Inactive
- Interface:** Shows the state of the main interface:
  - Entrée[Entree 1]: Inactive

## Wizard affiché dans les pages web à la première mise en service

FR

A la 1<sup>ère</sup> mise en service, un wizard vous invite à définir certaines règles de cybersécurité.

EN

Configuration du poste Restaurer les paramètres

Présentation générale

### Bienvenue

Votre poste sort d'usine, vous devez choisir quelle politique de sécurité vous souhaitez mettre en œuvre. Cette politique pourra être modifiée ultérieurement dans les paramètres systèmes du poste.

Par mesure de sécurité il est recommandé de choisir au moins une politique de sécurité de niveau modérée

Vous devez créer un 1er compte administrateur.

Il est conseillé d'effectuer une sauvegarde à la fin de la configuration complète du poste pour être en mesure de la restaurer en cas de perte du mot de passe administrateur.

J'ai lu et accepte les conditions générales

Suivant

Configuration du poste Restaurer les paramètres

Politique de sécurité (1/2)

Faible **Modérée** Forte Personnalisée

Complexité des mots de passe

	Faible	Modérée	Forte
Chiffrement des mots de passe	✓	✓	✓
Nombre minimum de caractères	1	6	10
Au minimum 1 chiffre/1 majuscule/1 c. spécial	✗	✓	✓
Compte utilisateur ≠ Mot de passe	✗	✓	✓
Mot de passe renouvelable	✗	✓	90 jours
Historique des mots de passe	1	1	10

Précédent Suivant

Configuration du poste Restaurer les paramètres

Politique de sécurité (2/2)

Faible **Modérée** Forte Personnalisée

Configuration du pare-feu et des services

Activer le pare-feu

Service web

HTTP

CastelSuite et connexion inter-équipements

Activer la connexion à CastelSuite et les connexion inter-équipements

Précédent Suivant

Configuration du poste Restaurer les paramètres

Création du compte administrateur

castel

\*\*\*\*\*

Confirmer le mot de passe

✗ Nombre minimum de caractères : 10  
 ✗ Nombre de lettres majuscules minimum : 1  
 ✗ Nombre de chiffres minimum : 1  
 ✗ Nombre de caractères spéciaux minimum : 1  
 ✗ Confirmer le mot de passe

ⓘ Toute perte de mot de passe entrainera une réinitialisation du poste en mode usine !

Précédent Suivant

En 1<sup>er</sup> lieu vous devez choisir le niveau de politique de sécurité qui influe :

- Sur le niveau de complexité des mots de passe qui sera appliquée à chaque création de compte et notamment pour le compte administrateur.
- Sur les règles de firewall. Selon le niveau choisi vous pouvez définir si vous activez ou non le firewall, maintenez la connexion web via le port http et si vous pouvez accéder à la configuration des équipements depuis le logiciel CastelSuite.

Ces paramètres peuvent ensuite être modifiés et complétés dans la page de configuration de la « Sécurité ».



**Lorsque vous avez fini de paramétrer votre poste, nous vous conseillons fortement de sauvegarder la configuration du poste. Cela vous permettra de restaurer votre équipement en cas de perte de vos identifiants.**

## ENTRETIEN

Le nettoyage de votre produit CASTEL doit être réalisé uniquement à l'aide d'un produit nettoyant doux non abrasif, non moussant et surtout exempt de tout type de solvant ou alcool..

Le nettoyage au jet est à proscrire, ainsi que les éponges abrasives et tissus à surface agressive.

## FONCTIONS

Le portier est conçu pour dialoguer avec tous les autres postes de la gamme Interphonie sur IP Castel (XELLIP, CAP IP ...), des Softphones, des téléphones SIP ou tout autre équipement compatible avec la norme SIP.

Le poste peut également établir une communication Audio avec les postes de la gamme numérique Castel. Ce type de communication nécessite l'utilisation d'une passerelle supplémentaire M-HYB-IP.

### Fonctions générales du portier

- Etablir une communication audio conformément à la norme SIP :
  - ↳ En point à point
  - ↳ En s'enregistrant sur un serveur SIP. Il est possible de définir plusieurs compte SIP, chacun ayant jusqu'à 2 serveurs de secours.

Avec prise en charge des protocoles de transport réseau UDP, TCP et TLS.
- Gestion des communications audios
  - ↳ Possibilité de définir le niveau de priorité du poste
  - ↳ Possibilité de définir le timeout d'appel et de communication
  - ↳ Avec ou sans décroché automatique, avec ou sans retard
  - ↳ Possibilité d'activer le mode secret sur décroché automatique
- Réglage de la date et de l'heure manuellement ou via un serveur NTP. Le poste peut également servir de serveur NTP.
- Interfaçage natif avec le contrôle d'accès Synchronic. Permet de régler les paramètres nécessaires au bon fonctionnement : gestion des certificats, configuration des accès...

### Fonctions sécurité & réseau

- Configuration de l'interface réseau avec au choix 1 ou 2 interfaces séparées ou en bridge et possibilité d'ajuster la vitesse de communication (10/100/1000Mbit/s)
- Prise en charge des VLAN
- Prise en charge du Spanning Tree Protocol pour gérer les boucles réseaux
- Possibilité d'activer une sécurisation des connexions Ethernet via le protocole 802.1X (RADIUS). Protocoles d'authentification pris en charge : EAP-TLS, EAP-TTLS, PEAP et EAP-MD5.
- Définition d'une politique de sécurité et mise en œuvre d'un firewall entraînant :
  - ↳ La définition de la complexité des mots de passe
  - ↳ Des restrictions dans l'utilisation des services (notamment la fermeture des ports non utilisés) avec possibilité de définir des règles de firewall personnalisées
  - ↳ La possibilité de restreindre l'accès aux services à des équipements par plage d'adresse IP

### Fonctions de l'interface audio

- Configurer le volume HP, le volume Micro et le volume de boucle auditive
- Configurer l'algorithme audio permettant notamment d'ajuster l'Anti Echo Acoustique (AEC), la réduction de bruit ambiant (NR) et la suppression d'écho acoustique (AES)
- Configurer les sonneries et les tonalités
- Configurer les paramètres de détection de bruit. Permet par exemple de déclencher un appel.
- Configurer les paramètres audios de communication : port RTP, codecs audios (PCMU / PCMA / GSM / G722 / G729)
- Configurer les commandes DTMF selon les protocoles RFC-2833 et SIPINFO. Permet par exemple d'enclencher un relais lors d'une communication.
- Basculer en simplex sur réception d'une commande DTMF (à partir du poste distant)
  - ↳ « \* » permet de basculer en simplex écoute
  - ↳ « # » permet de basculer en simplex parole
  - ↳ « 0 » permet de revenir en fonctionnement standard

### Fonctions des interfaces entrée TOR

- Configurer l'entrée de type ETAT ou COMPTEUR
- Configurer l'état actif de l'entrée : contact ouvert ou contact fermé
- Configurer une temporisation de prise en compte d'un changement d'état (fonction antirebonds)
- Configurer le seuil du compteur
- Inhiber l'entrée

## Fonctions des interfaces Sortie

- Configurer le type de sortie relais : monostable, bistable ou clignotant
- Configurer le type de contact : Normalement Ouvert ou Normalement Fermé
- Commander la sortie Marche/Arrêt
- Commander la sortie Forçage Ouvert/Fermé
- Configurer les paramètres temporels de la sortie

## Fonctions des entrées logiques (ou flags)

Les entrées logiques permettent deux fonctionnalités en particulier :

- De créer un état logique à partir duquel il est possible de conditionner des actions dans les relations.
- De créer un compteur qui est actualisé en fonction d'événements et en fonction de la valeur de ce compteur de déclencher éventuellement une ou plusieurs actions.

Le paramétrage des entrées logiques nécessite l'utilisation du logiciel CastelServeur.

## Configuration des relations

**Le serveur Web est le lieu de paramétrage des automatismes également appelés relations.**

Il existe deux types de relations :

- Horaire : permet de déclencher des actions sur des plages horaires identifiées. Il existe trois niveaux de priorité pour une relation horaire (Haute, Moyenne et Basse).
- Logique :
  - ↳ Condition logique : permet de déclencher des actions sur certaines conditions d'état (actif, inactif...). Une relation logique peut intégrer plusieurs conditions par des opérateurs tels que AND, OR, NOT, XOR. De même une relation logique peut déclencher plusieurs actions.
  - ↳ Condition numérique (Comptage) : permet d'effectuer des actions en comparant la valeur d'un compteur avec différents seuils. Il est également possible d'additionner ou soustraire des valeurs de compteurs et de comparer le résultat obtenu.

## Configuration des utilisateurs

Le serveur du poste permet de créer, modifier ou supprimer des utilisateurs.

Il existe plusieurs types d'utilisateurs :

- Web : les utilisateurs autorisés à se connecter et à exploiter les pages web de configuration du poste

Pour chaque utilisateur un identifiant et un mot de passe est demandé.

Pour les utilisateurs web, il est de plus possible :

- De définir la langue d'affichage lorsque l'utilisateur est connecté
- Les droits associés

## Configuration des profils

Il est possible de créer, modifier ou supprimer des profils de fonctionnement du poste. Chaque profil spécifie une priorité du poste et des droits d'accès au poste.

Le poste peut fonctionner avec un profil unique ou avec différents profils selon des plages horaires.

## Fonction SNMP (Simple Network Management Protocol)

Le poste intègre un agent SNMP permettant de répondre à des requêtes SNMP et d'envoyer des notifications (TRAPS) à un manager SNMP.

A partir des pages web, il est possible de :

- Configurer différentes communautés (lecture / écriture)
- Configurer des données système (sysContact et sysLocation)
- Configurer les notifications (destinataire, communauté...)
- Télécharger la MIB Castel

Les versions SNMPv1 et SNMPv2c sont supportées.

## Fonction notification ASCII

Le poste intègre un mécanisme de notification à travers des chaînes ASCII.

A partir des pages web, il est possible de :

- Configurer les paramètres pour se connecter à un serveur TCP distant et de préciser les caractéristiques de la connexion
- Configurer des événements permettant d'envoyer une trame ASCII vers ce serveur TCP



## Fonction autotest

Le poste dispose de plusieurs tests permettant de valider son fonctionnement :

- Autotest HP/MIC : permet de tester à distance le bon fonctionnement du HP et du micro. A partir de la page « paramètres avancés » il est possible d'adapter les niveaux de ce test suivant l'environnement d'installation. Ce test peut être déclenché à partir du serveur web ou par une commande SNMP. Le résultat du test est visible via l'historique du serveur web et par une notification SNMP.

## Fonction Fil de l'eau des événements

Le fil de l'eau permet de visualiser tous les événements survenus sur le poste. Ils sont répertoriés en faisant apparaître la date et l'heure de l'événement concerné ainsi que les informations associées.

## Fonction Journal d'appel

Le journal d'appel permet de visualiser simplement l'historique des événements de communication : appels reçus, appels émis, communications établies et transferts ou renvois d'appel.

## Fonction de sécurité

Le journal de sécurité permet de visualiser simplement l'historique des événements de sécurité survenus sur le poste : Les événements d'authentification, liés au compte utilisateur ou à la politique de sécurité.

## Sauvegarde et restauration des paramètres du système

Il est possible de réaliser une sauvegarde ou une restauration complète des paramètres du poste (configuration, profils, relations, annuaire...)

Il est possible de remettre le poste en configuration usine en appuyant pendant 10s sur le bouton reset au moment du démarrage du poste.

## Mise à jour du poste

Il est possible de mettre à jour le poste en envoyant un fichier contenant la nouvelle version logicielle.

Le poste redémarre ensuite automatiquement afin d'appliquer la mise à jour. La mise à jour ne modifie en aucun cas les paramètres utilisateur.

## Sauvegarde sur coupure d'alimentation

Lorsqu'une coupure d'alimentation survient, le poste est capable de sauvegarder les éléments suivants :

- Les valeurs des compteurs
- L'historique
- Les événements secourus (ces événements sont définis à partir de CastelServeur)
- Les états des interfaces

## CARACTERISTIQUES TECHNIQUES

FR

EN

### Conformités aux directives européennes

- 2001/95/EC : Sécurité
- 2014/30/UE : CEM
- 2017/2102/UE : RoHS 3
- 2014/35/UE : Basse Tension

### Conformités aux normes européennes

- EN 55032 : Emissions CEM
- EN 55035 : Immunité CEM
- EN 55024 : Immunité CEM
- EN 62368-1 : Sécurité des personnes – Sécurité électrique
- EN 61000-6-1, 4-2, 4-3, 4-4 : Immunité CEM
- EN 61000-6-3 : Emissions CEM

### Caractéristiques mécaniques

- Degré de protection IP65 selon EN 60529
- Indice de résistance IK08 selon EN 62262
- Face avant désinfectable et bactéricide
- Face avant et fond encastrable en ABS
- Dimensions : H 280 x L 145 x P65 mm
- Poids : 1,2kg

### Caractéristiques électriques générales

- Température de fonctionnement : -20° à +50°C
- Température de stockage : -20° à +70°C
- Humidité relative : <90%, sans condensation
- Alimentation auxiliaire :
  - ↳ 24VDC (20 à 30VDC) 30W max
- Alimentation PoE IEEE 802.3af 12,9W max
- Alimentation PoE+ IEEE 802.3at 25,5W max
- Consommation au démarrage : 10W
- Consommation au repos : 4W
- Consommation max : 21W

### Entrées

- 2 entrées TOR protégées et filtrées
- Vitesse d'acquisition 5Hz (200ms)

### Sorties

- 2 sorties relais libres de potentiel
- Pouvoir de coupure du relais 42,4VAC/60 VDC/5A/150VA
- La fréquence maximale est de 5Hz (temps de commutation minimum : 200ms)

### Audio

Puissance sonore maximale :

- Si alimentation PoE+ : 4W
  - ↳ LAeq 78dB @1m (bruit rose)
  - ↳ LAeq 85dB @1m (sinusoïde 1000Hz)

Fréquence d'échantillonnage : 16KHz

Codecs : G711 Ulaw et Alaw / GSM / G722 / G729

### DTMF

- RFC-2833
- SIP INFO

### Sécurité & Réseau

- PoE conformité norme IEEE 802.3af
- PoE+ conformité norme IEEE 802.3at
- Ethernet 10/100/1000 Mbit sur 1, 2 interfaces ou en bridge, avec support des VLAN
- Support du protocole 802.1X (RADIUS)
- Support du Spanning Tree Protocol
- Prise en charge SNMP v1 et v2c
- Intègre divers mécanismes de sécurisation logiciels dont :
  - ↳ Firewall avec possibilité de lister les services & ports actifs
  - ↳ Politique de sécurité adaptative
  - ↳ Restriction par adresse IP



#### Protection de l'environnement :

Éliminez ce produit conformément aux règlements sur la préservation de l'environnement.



## PRESENTATION

### Product : 595.0000 (XE2 MED TOUCH)

Your SIP intercom equipment offers the following features:

- Establish an audio communication with Castel IP intercom stations, softphones, or any other equipment compatible with the SIP standard:
  - ↳ Point to point
  - ↳ By registering on a SIP server with the possibility of configuring up to 2 backup servers and multi SIP accounts
- Establish audio communication with Castel digital and analogue stations (requires additional M-HYB-IP gateway)
- Embedded web server for configuration and operation from any browser
- Embedded cybersecurity mechanisms, including :
  - ↳ Firewall with listing of active services and ports
  - ↳ Security policy applied to users and external services
  - ↳ IP range restriction
  - ↳ Securing Ethernet connections via the 802.1X protocol (RADIUS)
- Management of profiles, selectable by time slot or via automatism
- Management of advanced automatism (logical and time relations) on its interfaces
- Support for the following services:
  - ↳ SNMP (Simple Network Management Protocol)
  - ↳ Notification to supervisors via ASCII strings
- Native interfacing with the Synchronic access control solution
- Self-tests that can be run automatically or on demand
- Support for the following languages: French / English / Spanish / Polish / Dutch



It has the following features:

- 7-inch touch screen
- 2 "All or Nothing" inputs
- 2 dry contacts to control a door striker or other equipment
- External power supply, PoE (Power Over Ethernet) or PoE+ (Power Over Ethernet Plus)
- 2 x 10/100/1000MB Ethernet ports allowing 1 bridge connection (allows connection to another IP system) +VLAN support.

## CONNECTION

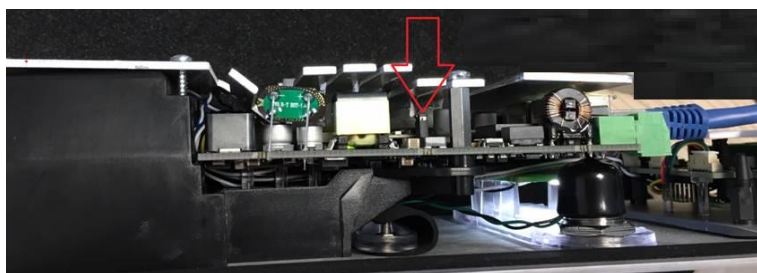
### Power supply connection (24VDC)

The required power supply is 20 to 30VDC.

Note: The intercom can be powered by the Ethernet network in PoE+ or PoE (with some restrictions)

Your intercom is delivered from the factory in PoE/PoE+ configuration, however in some cases it may be necessary to block it in a PoE only configuration (distribution of the Switch's power to several intercoms/ poor management of the Switch's power supply/ ...).

In this case with the intercom not powered and with a small non-conductive pliers, remove the strap indicated in red on the picture below



### IP network connection (ETH0 / ETH1)

The connection is made via an Ethernet 10/100/1000 Mbits RJ45 class 5e or 6 link.

2 Ethernet ports are available (1 PoE or PoE+ compatible and 1 non-PoE)

### Connection of the 0dB output (0dB +/-) *Applicable from software version 1.5.0*

A 0dB **differential** output allows the connection of an external amplifier.

+ : Hot spot

- : Cold spot

0V: Ground

### RS485 VDIP bus connection (RS1 / RS2 / 0V) *Configurable via CASTELSuite*

The intercom can manage up to 4 VDIP peripherals (VD4S ref 110.1000, VD8EI ref 110.1100, VDLECT ref 110.1200) via an RS485 bus line (bus wiring: several peripherals are installed on the same bus line).

The bus connection between the peripherals and the intercom is made via the points RS1, RS2 (via a twisted pair) and the earth. Establish the point-to-point connection by respecting the order of the signals.

The maximum length of the bus is 1Km. It is necessary to install a 120Ω resistor (supplied with the device) between the RS1 and RS2 points at each end of the bus.

### Connection of inputs (IN1 / IN2 / 0V)

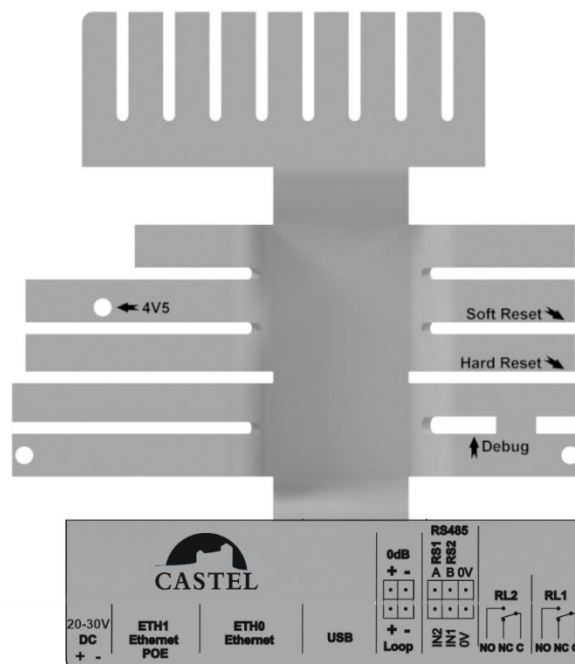
Two digital inputs allow the connection of a dry contact (do not apply voltage). To be activated, the input must be connected to the earth.

The contact can be moved up to 1 km.

### Connection of relay outputs (RL1 / RL2)

The connection is made via a 3-point terminal block providing the "Common (C) / Rest (NC) / Work (NO)" interface.

If you are using one of these relay outputs to control an AC or DC door striker, wire a non-biased 58V diode in parallel on the dry contact between C and NO or C and NC depending on use (diode supplied).



## INSTALLATION

FR

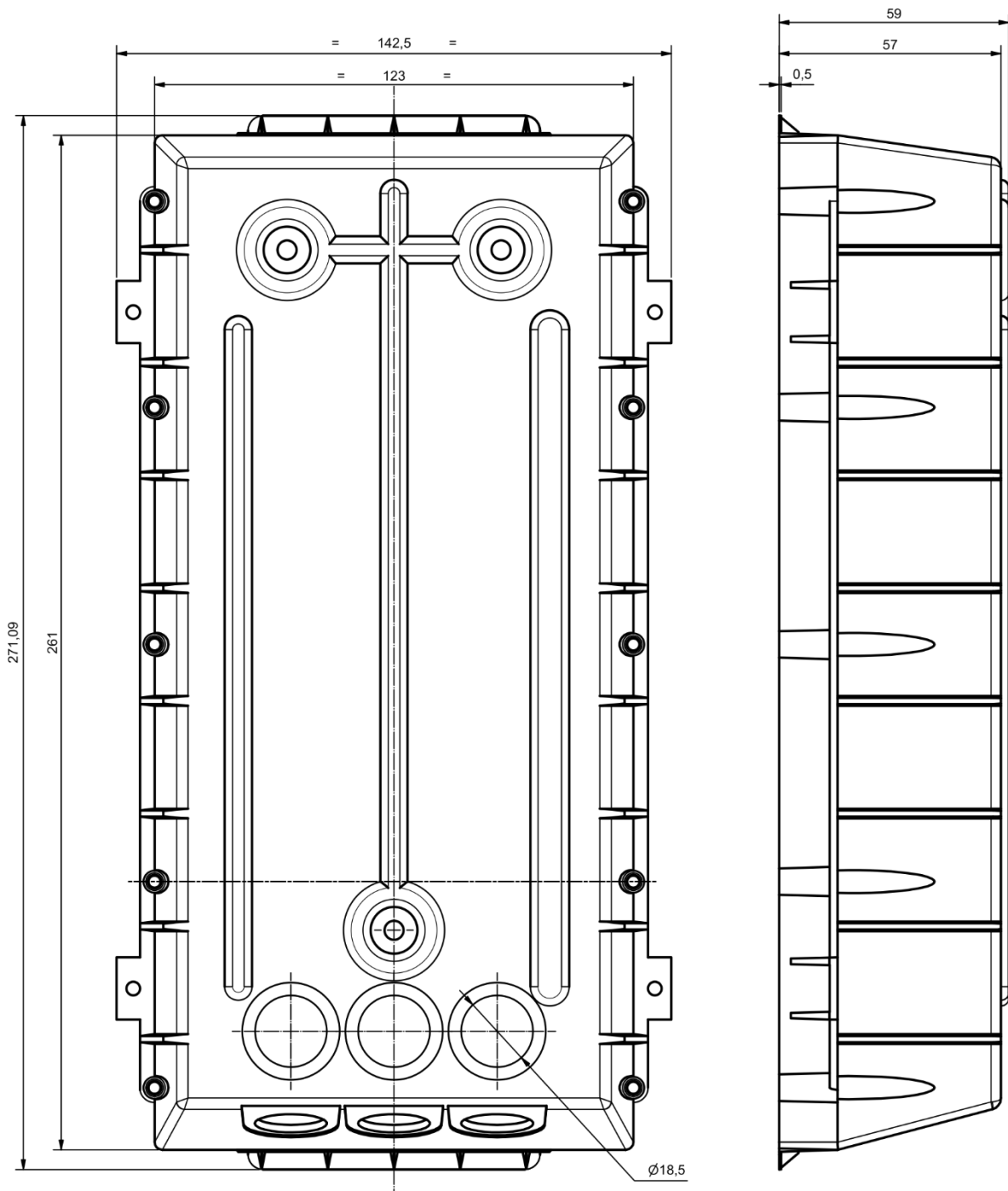
EN

### Flush mounting

- Make a recess in the support with a minimum dimension of 266mm high, 145mm wide and 64mm deep.
- Coat the bottom of the recess with at least 10mm of fresh cement.
- Insert the bottom of the intercom into the recess and push, pressing the flush-mounted socket against the support where the recess was made.
- Allow the cement to dry for at least 24 hours, then connect the intercom.
- Position and clip the plate onto the base.

### Flush mounting on plasterboard

- Make a recess in the support with a minimum dimension of 266mm high and 145mm wide.
- For mounting on BA13 (plasterboard), use the clamps provided, then connect the intercom.
- Position and clip the plate onto the base.





To remove the board, use a flat screwdriver to insert the tip into the slot provided in the lower part of the board, then rotate the screwdriver and pull manually to unclip the board from its support.

## USE

### IP address of the station

The workstation is delivered by default in DHCP. If there is no DHCP server, the workstation gets a fixed IP address from the IPV4LL domain: 169.254.xx.xx.

The IP address (static IP) and other network parameters can be set by changing the configuration of the workstation.

The discovery of the IP address of the station is possible from :

- CastelIPSearch software
- CastelServeur software

If the discovery of the IP address of the station is not possible :

- In factory configuration, the station states its IP address when the 1st<sup>st</sup> programmable button is pressed
- The station also states its IP address when the "Soft Reset" push button on the electronic board is briefly pressed
- By pressing and holding the "Soft Reset" button for more than 3 seconds, the station sets the IP address to 192.168.49.251.

### Reset of the station

Pressing and holding the "Soft Reset" push button for more than 20 seconds will restart the station and reset the parameters to the factory settings.

Pressing the "Hard Reset" button only causes the station to restart immediately.

### Access to the Station Web Server

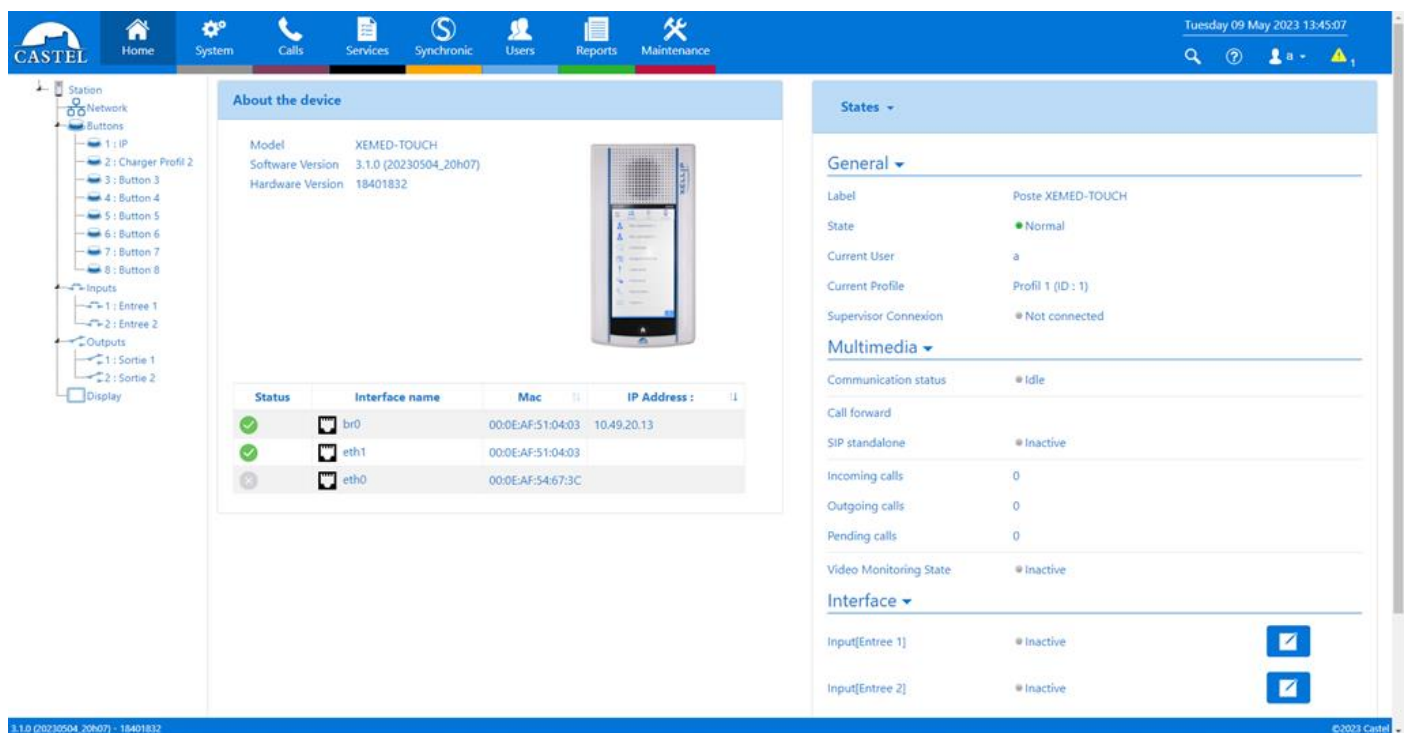
Access to the station's web server is possible from a browser such as Chrome, Edge or Firefox.

Open your browser from a device on the same network and type: **https://[workstation\_ip\_address]**

Then 2 situations are possible:

- Either your station is in factory configuration, a wizard must be filled in before any other operation
- Or your computer already has a configuration. Please enter the login and password that have been defined by the site administrator.

Please note: online help is available from all menus. This help provides information on the various functions of the web server.



The screenshot displays the web interface for the XE2 MED TOUCH station. The top navigation bar includes icons for Home, System, Calls, Services, Synchronic, Users, Reports, and Maintenance. The main content area is divided into several sections:

- Station Overview:** A tree view on the left shows the station's structure, including Network, Buttons (1-8), Inputs (Entree 1-2), Outputs (Sortie 1-2), and Display.
- About the device:** A central panel displays device details:
  - Model: XEMED-TOUCH
  - Software Version: 3.1.0 (20230504\_20h07)
  - Hardware Version: 18401832
- Network Table:** A table below the device info shows network interfaces:
 

Status	Interface name	Mac	IP Address
✓	br0	00:0E:AF:51:04:03	10.49.20.13
✓	eth1	00:0E:AF:51:04:03	
✗	eth0	00:0E:AF:54:67:3C	
- States:** A right-hand panel shows the station's status:
  - Label: Poste XEMED-TOUCH
  - State: Normal
  - Current User: a
  - Current Profile: Profil 1 (ID : 1)
  - Supervisor Connexion: Not connected
  - Communication status: Idle
  - Call forward: Inactive
  - SIP standalone: Inactive
  - Incoming calls: 0
  - Outgoing calls: 0
  - Pending calls: 0
  - Video Monitoring State: Inactive
  - Interface: Input[Entree 1] and Input[Entree 2] are both Inactive.

## Wizard displayed in the web pages at first start-up

At the first start-up, a wizard prompts you to define certain cybersecurity rules.

**Security policy (1/2) Password complexity table:**

	Low	Moderate	High
Password encryption	✓	✓	✓
Minimum number of characters	1	6	10
At least 1 digit/1 capital letter/1 special letter	✗	✓	✓
User account ≠ Password	✗	✓	✓
Renewable password	✗	✗	90 days
Password history	1	1	10

First, you must choose the level of security policy that affects :

- The level of complexity of the passwords which will be applied to each account creation and in particular for the administrator account.
- The firewall rules. Depending on the level you choose you can define if you activate or not the firewall, maintain the web connection via the http port and if you can access the equipment configuration from the CastelSuite software.

These settings can then be modified and completed in the "Security" configuration page.



**When you have finished setting up your workstation, we strongly advise you to save the workstation configuration. This will allow you to restore your equipment if you lose your identifiers.**

## MAINTENANCE

Your CASTEL product should only be cleaned with a mild, non-abrasive, non-foaming cleaning product that is free of any type of solvent or alcohol. Cleaning with a hose should be avoided, as well as abrasive sponges and fabrics with aggressive surfaces.



## FUNCTIONS

The intercom is designed to dialogue with all other stations in the Castel IP Intercom range (XELLIP, CAP IP ...), softphones, SIP phones or any other equipment compatible with the SIP standard.

The station can also establish an Audio communication with the Castel digital range. This type of communication requires the use of an additional M-HYB-IP gateway.

### General doorkeeper functions

- Establish an audio communication according to the SIP standard:
  - ↳ Point to point
  - ↳ By registering on a SIP server. It is possible to define several SIP accounts, each with up to 2 backup servers.

With support for UDP, TCP and TLS network transport protocols.

- Audio communication management
  - ↳ Possibility to define the priority level of the position
  - ↳ Possibility to define the call and communication timeout
  - ↳ With or without automatic pick-up, with or without delay
  - ↳ Possibility to activate the secret mode on automatic pick-up
- Setting the date and time manually or via an NTP server. The station can also be used as an NTP server.
- Native interfacing with Synchronic access control. Allows you to set the parameters necessary for proper operation: certificate management, access configuration, etc.

### Security & network functions

- Configuration of the network interface with a choice of 1 or 2 separate or bridge interfaces and the possibility to adjust the communication speed (10/100/1000Mbit/s)
- VLAN support
- Support for Spanning Tree Protocol to manage network loops
- Option to enable secure Ethernet connections via 802.1X (RADIUS). Supported authentication protocols: EAP-TLS, EAP-TTLS, PEAP and EAP-MD5.
- Definition of a security policy and implementation of a firewall resulting in :
  - ↳ The definition of password complexity
  - ↳ Restrictions on the use of services (including closing unused ports) with the possibility of defining custom firewall rules
  - ↳ The ability to restrict access to services to equipment by IP address range

### Audio interface functions

- Setting the speaker volume, microphone volume and hearing loop volume
- Configure the audio algorithm to adjust Acoustic Echo Cancellation (AEC), Ambient Noise Reduction (NR) and Acoustic Echo Suppression (AES)
- Setting up ringtones and tones
- Configure noise detection settings. For example, to trigger a call.
- Configure audio communication parameters: RTP port, audio codecs (PCMU / PCMA / GSM / G722 / G729)
- Configure DTMF commands according to RFC-2833 and SIPINFO protocols. Allows, for example, to switch on a relay during a communication.
- Switch to simplex on receipt of a DTMF command (from the remote station)
  - ↳ "\*" toggles to simplex listening
  - ↳ "#" toggles to simplex speech
  - ↳ "0" returns to standard operation

### Functions of the digital input interfaces

- Configuring the STATUS or COUNTER input
- Configure the active state of the input: contact open or contact closed
- Configuring a time delay to take into account a change of state (anti-bounce function)
- Setting the counter threshold
- Inhibiting entry

## Output interface functions

- Configure the type of relay output: monostable, bistable or flashing
- Configure contact type: Normally Open or Normally Closed
- Controlling the On/Off output
- Controlling the Forcing Open/Closed output
- Configuring the time parameters of the output

## Logic input functions (or flags)

Logic inputs allow two features in particular:

- To create a logical state from which to condition actions in relationships.
- Create a counter that is updated according to events and, depending on the value of this counter, possibly trigger one or more actions.

The setting of the logic inputs requires the use of CastelServeur software.

## Configuration of relationships

**The web server is the place where the automatisms, also called relations, are set up.**

There are two types of relationships:

- Schedule: Allows actions to be triggered on identified time slots. There are three levels of priority for a time relationship (High, Medium and Low).
- Logic:
  - ↳ Logical condition: allows actions to be triggered on certain state conditions (active, inactive, etc.). A logical relation can integrate several conditions by operators such as AND, OR, NOT, XOR. In the same way a logical relation can trigger several actions.
  - ↳ Numerical condition (Counting): Allows actions to be performed by comparing the value of a counter with different thresholds. It is also possible to add or subtract counter values and compare the result.

## User configuration

The workstation server allows users to be created, modified or deleted.

There are several types of users:

- Web: users who are allowed to log in and use the workstation configuration web pages

For each user a login and a password is required.

For web users, it is also possible to :

- Define the display language when the user is logged in
- Associated rights

## Profile configuration

It is possible to create, modify or delete workstation operating profiles. Each profile specifies an asset priority and asset access rights.

The station can work with a single profile or with different profiles according to time slots.

## SNMP (Simple Network Management Protocol) function

The station has an SNMP agent to respond to SNMP requests and to send notifications (TRAPS) to an SNMP manager.

From the web pages, it is possible to :

- Configure different communities (read/write)
- Configure system data (sysContact and sysLocation)
- Configure notifications (recipient, community...)
- Download the Castel MIB

SNMPv1 and SNMPv2c versions are supported.

## ASCII notification function

The station incorporates a notification mechanism through ASCII strings.

From the web pages, it is possible to :

- Configure settings to connect to a remote TCP server and specify the characteristics of the connection
- Set up events to send an ASCII frame to this TCP server

## Self-test function

The station has several tests to validate its operation:

- SPEAKER/MIC self-test: Allows you to remotely test the correct operation of the speaker and the microphone. From the "advanced settings" page it is possible to adapt the levels of this test according to the installation environment. This test can be triggered from the web server or by an SNMP command. The result of the test is visible via the web server history and an SNMP notification.

## Event flow function

The flow chart allows you to view all the events that have occurred on the station. They are listed with the date and time of the event concerned and the associated information.

## **Call log function**

---

The call log provides a simple way to view the history of communication events: calls received, calls made, calls established and call transfers or forwarding.

## **Safety function**

---

The security log provides a simple way to view the history of security events that have occurred on the computer: authentication events, events related to the user account or the security policy.

## **Backing up and restoring system settings**

---

It is possible to carry out a backup or a complete restoration of the station parameters (configuration, profiles, relations, directory...)

It is possible to reset the station to factory configuration by pressing the reset button for 10s when the station is started.

## **Updating the position**

---

It is possible to update the station by sending a file containing the new software version.

The workstation will then automatically restart to apply the update. The update does not change the user settings in any way.

## **Backup on power failure**

---

When a power cut occurs, the post is capable of saving the following items:

- The values of counters
- The history
- The events supported (these events are defined at from from CastelServeur)
- The states of the interfaces

## TECHNICAL CHARACTERISTICS

FR

EN

### Compliance with European Directives

- 2001/95/EC: Safety
- 2014/30/UE: CEM
- 2017/2102/EU: RoHS 3
- 2014/35/EU: Low Voltage

### Compliance with European standards

- EN 55032: EMC emissions
- EN 55035: EMC immunity
- EN 55024: EMC immunity
- EN 62368-1: Personal safety - Electrical safety
- EN 61000-6-1, 4-2, 4-3, 4-4: EMC immunity
- EN 61000-6-3: EMC emissions

### Mechanical characteristics

- Protection class IP65 according to EN 60529
- Resistance class IK08 according to EN 62262
- Disinfectable and bactericidal front panel
- ABS front and bottom panel
- Dimensions : H 280 x W 145 x D 65 mm
- Weight : 1.2kg

### General electrical characteristics

- Operating temperature : -20° to +50°C
- Storage temperature: -20° to +70°C
- Relative humidity: <90%, non-condensing
- Auxiliary power supply :
  - ↳ 24VDC (20 to 30VDC) 30W max
- IEEE 802.3af PoE power supply 12.9W max
- IEEE 802.3at PoE+ power supply 25.5W max
- Power consumption at start-up: 10W
- Power consumption at rest : 4W
- Maximum power consumption: 21W

### Inputs

- 2 protected and filtered digital inputs
- Acquisition speed 5Hz (200ms)

### Outputs

- 2 potential-free relay outputs
- Switching capacity of the relay 42.4VAC/60 VDC/5A/150VA

- The maximum frequency is 5Hz (minimum switching time: 200ms)

### Audio

- If PoE+ power supply: 4W
  - ↳ LAeq 78dB @1m (pink noise)
  - ↳ LAeq 85dB @1m (1000Hz sine wave)

Sampling frequency: 16KHz

Codecs: G711 Ulaw and Alaw / GSM / G722 / G729

### DTMF

- RFC-2833
- SIP INFO

### Security & Network

- PoE compliance with IEEE 802.3af standard
- PoE+ compliant with IEEE 802.3at standard
- Ethernet 10/100/1000 Mbit on 1, 2 or bridge interfaces, with VLAN support
- 802.1X (RADIUS) protocol support
- Spanning Tree Protocol support
- SNMP v1 and v2c support
- Incorporates various software security mechanisms including:
  - ↳ Firewall with possibility to list active services & ports
  - ↳ Adaptive security policy
  - ↳ Restriction by IP address



#### Environmental protection:

Dispose of this product in compliance with the environmental protection regulations.