

## PRESENTATION

### Références produits: 590.0050 (XE AUDIO 1B TRAM MODELE1)

Votre équipement d'interphonie SIP propose les fonctionnalités suivantes :

- Etablir une communication audio/vidéo 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 :
  - ↳ ONVIF (Open Network Video Interface Forum)
  - ↳ RTSP (Real Time Streaming Protocol)
  - ↳ 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 :

- 1 bouton d'appel programmable pour configurer des actions au choix
- 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.

## OPTIONS

- Référence 590.9220 : Ceinture
- Référence 590.9400 : Casquette
- Référence 590.9600 : Kit griffes (Montage sur placoplâtre)

## RACCORDEMENT

FR

EN

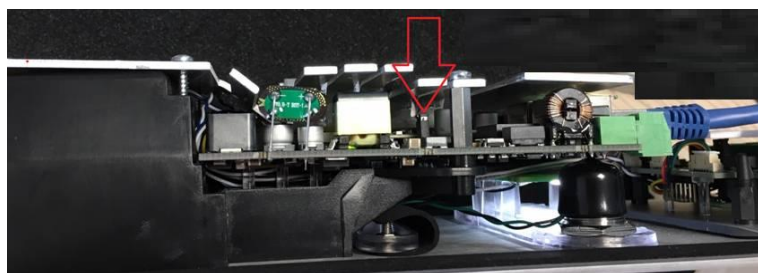
### Raccordement de l'alimentation (24VDC)

L'alimentation requise est de 20Vdc 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 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 de la sortie boucle induction magnétique (Loop)

Une sortie Loop permet le raccordement de la boucle d'induction magnétique.

### 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.

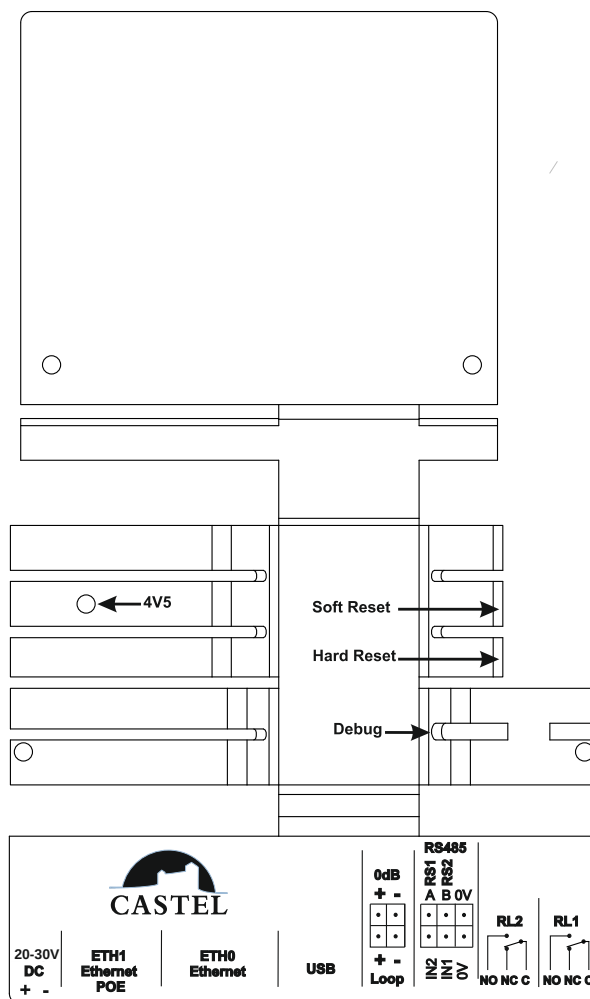
### Raccordement des sorties relais (RL1 / RL2)

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).

### Protection contre les décharges électrostatiques

Raccorder le portier à la terre en utilisant la cosse jaune fournie dans le sachet puis la connecter sur la fixation prévue située à côté du micro.



## INSTALLATION

FR

### Montage en encastrément

Faire une réservation hauteur 271mm, largeur 143mm et profondeur 61mm dans le support.

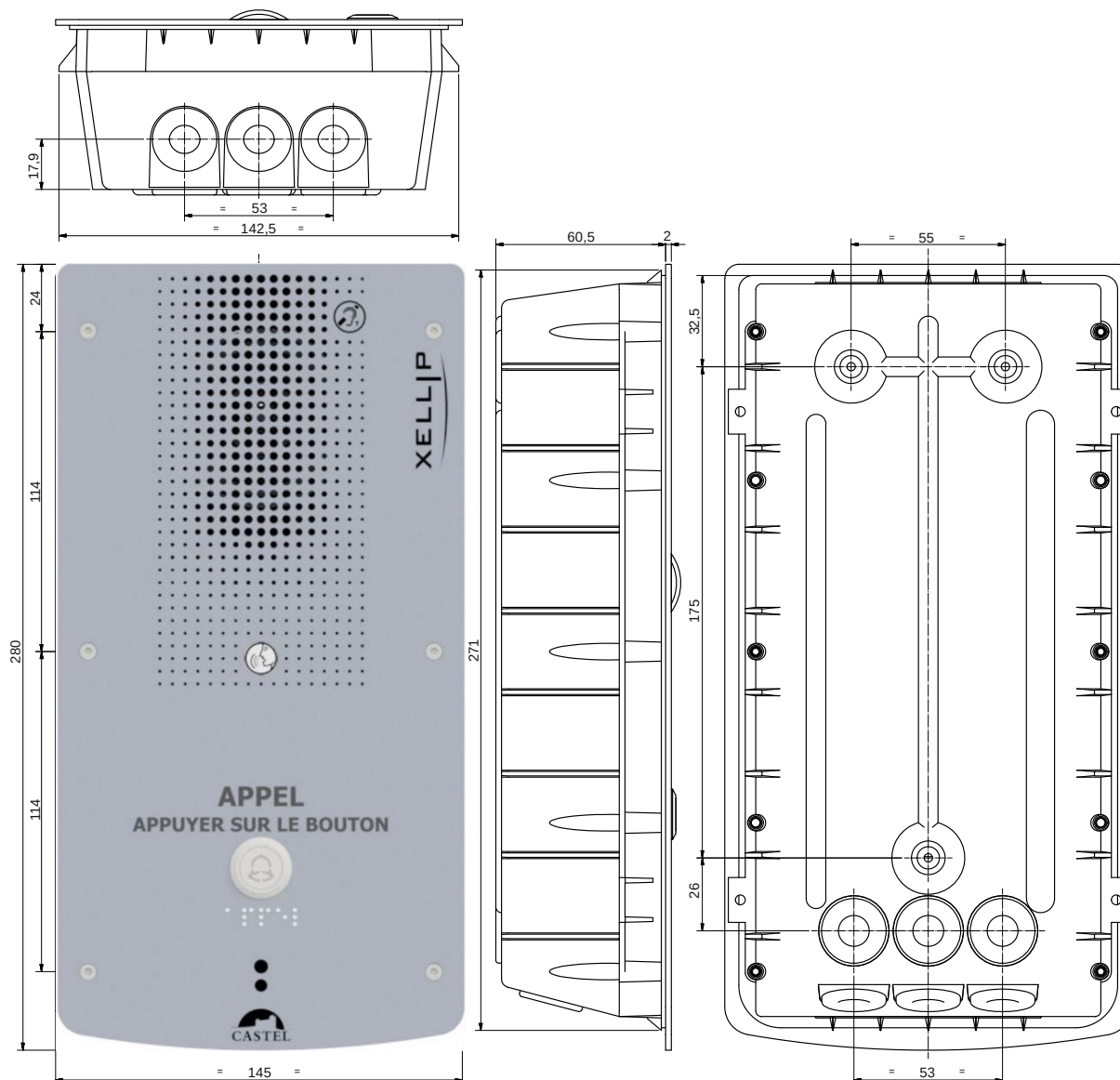
Monter le fond dans la réservation puis raccorder le portier.

Fixer la face avant avec les 6 vis FX (TORX) à téton M3 x 10.

EN



Ne pas encastrer trop profondément le fond car lors du montage de la face avant, le joint d'étanchéité de celle-ci ne serait plus en contact avec celui-ci. Ceci entraînant une rupture de l'étanchéité.



### Montage sur cloison en Placoplatre

Faire une réservation hauteur 266mm, largeur 143mm dans la cloison.

Monter le kit griffe (Option réf. 590.9600) sur fond du portier.



Fixer le fond du portier dans la réservation à l'aide des griffes puis raccorder le portier.

Fixer la face avant avec les 6 vis FX (TORX) à téton M3 x 10.

## Montage en saillie

Fixer le fond encastrable sur la ceinture (option réf. 590.9220) à l'aide des 4 vis CZ M3 x 6.

Fixer l'ensemble (fond + ceinture) sur son support par trois vis de diamètre 3 à 3,5 maxi.

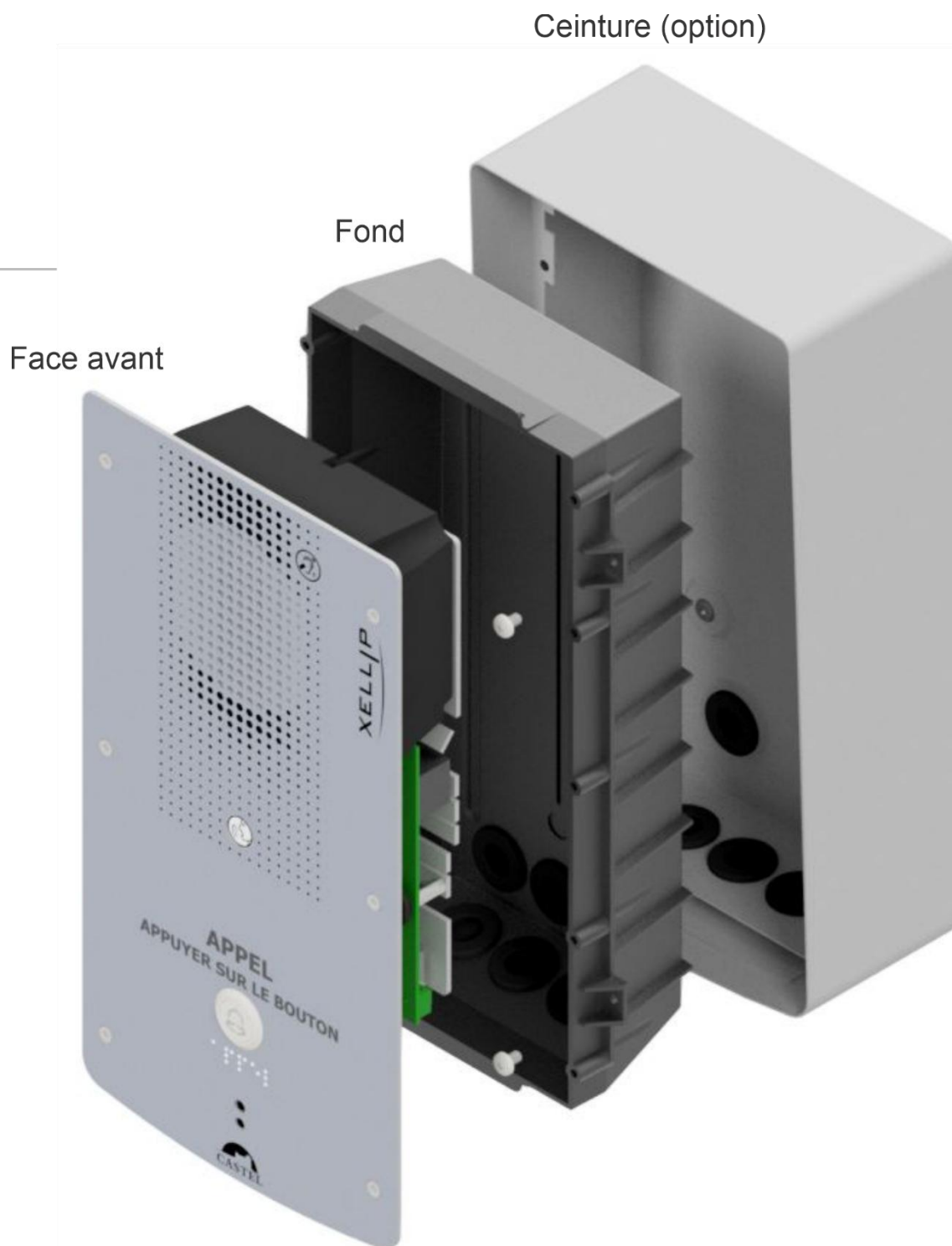
Raccorder le portier.

Fixer la face avant avec les 6 vis FX (TORX) à téton M3 x 10.

Pour garantir à votre portier une bonne étanchéité, il est nécessaire que la face avant une fois montée, appuie sur la totalité du joint d'étanchéité situé entre le fond et la face avant.

FR

EN



## Montage de l'option casquette

Casquette en inox 316L. Dimensions: 275 x 147 x 27 mm

Encastrer le fond.

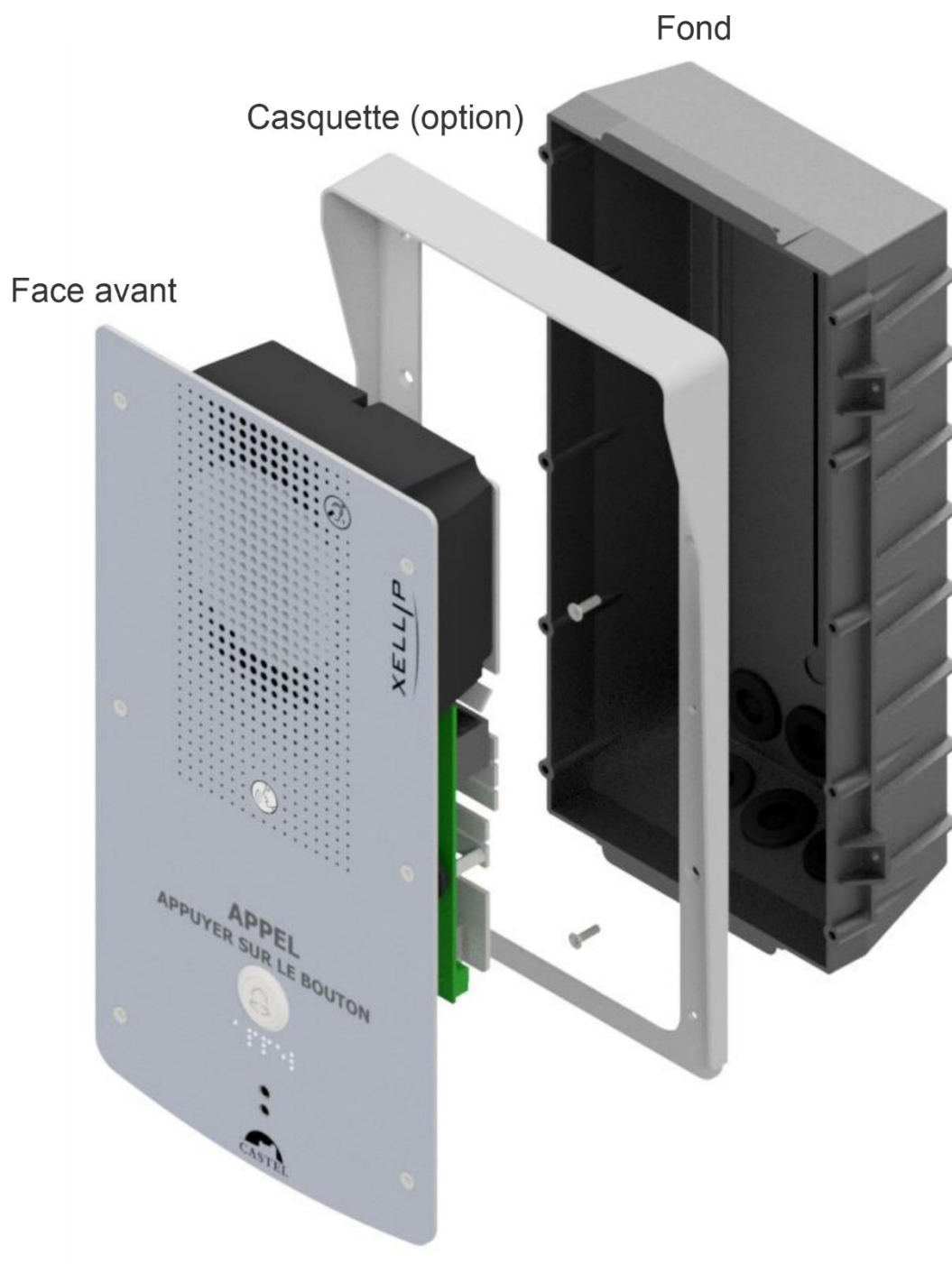
Fixer la casquette (Option réf. 590.9400) sur le fond encastrable à l'aide des 4 vis FX (TORX) M3-10.

Raccorder le portier.

Fixer la face avant avec les 6 vis FX (TORX) à béton M3 x 10.

FR

EN



**Montage sur potelet**

Usiner l'ouverture sur le potelet suivant le plan ci-après.

Raccorder le portier.

Fixer la face avant sur le potelet avec les 6 vis FX (TORX) à béton M3 x 10.

**ATTENTION!!! Le portier étant monté sans son fond, le potelet doit impérativement être étanche (IP 65).**





## UTILISATION

FR

EN

### 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 CastelIPSearch
- Le logiciel CastelServeur
- Tout logiciel de découverte ONVIF

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

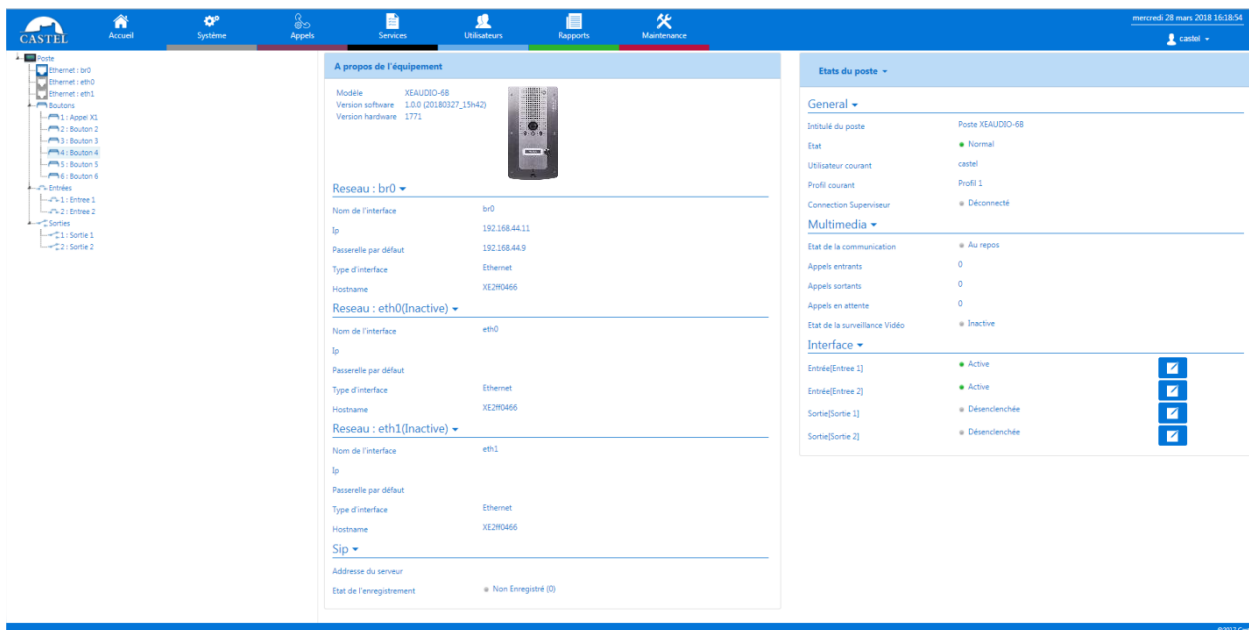
L'accès au serveur Web du poste est possible depuis un navigateur tel que Chrome, Edge ou Firefox.

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 Castel Web Server interface. The top navigation bar includes links for Accueil, Système, Appels, Services, Utilisateurs, Rapports, and Maintenance. The main content area is divided into several sections:

- A propos de l'équipement:** Displays the device model (XE AUDIO 1B), software version (1.0.0 (20180327\_15h42)), and hardware version (1771).
- Reseau:** Shows network configuration for three interfaces: br0 (IP: 192.168.44.11), eth0 (Inactive), and eth1 (Inactive).
- Etat du poste:** Provides a summary of the device's status, including the current state (Normal), user (castel), and connection status (Déconnecté).
- Interface:** Lists the status of various interfaces, such as Entrée (Active) and Sortie (Inactive).

The interface is designed with a clean, professional layout, using a blue and white color scheme. The left sidebar contains a tree view of the configuration options.

## 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 (eau ou eau savonneuse), non abrasif, non moussant et surtout exempt de tout type de solvant ou alcool.

Pour l'entretien courant, utilisez uniquement de l'eau, sans détergent.

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



## FONCTIONS

FR

EN

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/vidéo 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 et vidéos (selon la version)
  - ↳ 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 du bouton programmable

Le bouton est programmable et permet de :

- Faire un appel de 1 à 10 postes simultanés ou temporisés
- Commander le relais local, le relais du poste en communication ou d'envoyer un code DTMF
- Terminer une communication
- Exécuter une liste d'actions avancées

### 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

FR

EN

### 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
- RTSP : les utilisateurs pouvant exploiter le service de streaming audio/vidéo du poste
- ONVIF : les utilisateurs pouvant exploiter le service ONVIF 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, une configuration des boutons de fonctions et des droits d'accès au poste.

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

### Fonction ONVIF (Open Network Video Interface Forum)

Le poste est compatible avec le protocole ONVIF.

A partir des pages web, il est possible d'activer ou désactiver la découverte ONVIF.

Il est possible de configurer les scopes.

### Fonction RTSP (Real Time Streaming Protocol)

Le poste intègre un serveur RTSP permettant à un client RTSP externe de récupérer le flux audio et/ou vidéo du poste.

Un mécanisme d'authentification peut être activé pour sécuriser l'accès au flux.

Il est possible de définir les paramètres souhaités pour le flux mis à disposition.

## 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.
- Autotest des boutons mécaniques : la détection d'un bouton mécanique bloqué (contact présent pendant plus de 20s) est signalée par une notification SNMP et un événement est signalé dans l'historique du serveur web.

## 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

- Conception anti-vandale IK07 selon EN 62262
- Degré de protection IP65 selon EN 60529
- Face avant en inox 316L
- Fond encastrable en ABS avec accrochage mural
- Dimensions: H 280 x L 145 x P 63 mm
- Poids : 1,4kg

### 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 (20V à 30V) 30Watt max
- Alimentation PoE IEEE 802.3af 12,9Watt max
- Alimentation PoE IEEE 802.3at 25,5Watt max

### Boutons

- Vitesse d'acquisition 5Hz (200ms)

### Entrées

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

### Sorties

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

### Audio

Puissance sonore maximale :

- Si alimentation PoE : 1W
  - ↳ LAeq 78,5dB @1m (bruit rose)
  - ↳ LAeq 87dB @1m (sinusoïde 1000Hz)
- Si alimentation PoE+ : 6W
  - ↳ LAeq 85dB @1m (bruit rose)
  - ↳ LAeq 90dB @1m (sinusoïde 1000Hz)
- Si alimentation externe : 10W
  - ↳ LAeq 85,7dB @1m (bruit rose)
  - ↳ LAeq 91dB @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

### Utilisation

Pour une communication optimum, la distance entre le poste et l'interlocuteur ne doit pas dépasser 1m.



#### Protection de l'environnement :

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



## PRESENTATION

### Product reference: **590.0050 (XE AUDIO 1B TRAM MODEL1)**

Your SIP intercom equipment offers the following features:

- Establish 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 back-up servers and SIP multi-accounting.
- Establish audio communication with Castel's digital and analogue range of intercom stations (requires the use of an additional M-HYB-IP gateway)
- Includes a Web server for configuration and operation from any browser
- Embeds cybersecurity mechanisms, including:
  - ↳ Firewall with listing of active services and ports
  - ↳ Security policy applied to users and external services
  - ↳ IP range restriction
  - ↳ Secure Ethernet connections via 802.1X protocol (RADIUS)
- Profile management, selectable by time slot or via automations
- Management of advanced automations (logical and time relations) on its interfaces
- Support for the following services :
  - ↳ ONVIF (Open Network Video Interface Forum)
  - ↳ RTSP (Real Time Streaming Protocol)
  - ↳ SNMP (Simple Network Management Protocol)
  - ↳ Notification to supervisors via ASCII strings
- Native interfacing with the Synchronic access control solution
- Self-tests can be run automatically or on demand
- Support for the following languages French / English / Spanish / Polish / Dutch



It has the following features:

- 1 programmable call buttons for configuring actions of your choice
- 2 "On/Off" inputs
- 2 dry contacts to control a strike or other equipment
- External power supply, PoE (Power Over Ethernet) or PoE+ (Power Over Ethernet Plus)
- 2 Ethernet 10/100/1000MB ports for 1 bridge connection (enables connection of another IP system) + VLAN support.

## OPTIONS

- Reference 590.9220: Belt
- Reference 590.9400: Cap
- Reference 590.9600: Claw kit (plasterboard mounting)

## CONNECTION

FR

EN

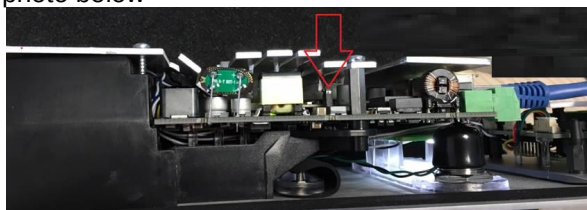
### Power supply connection (24VDC)

The required power supply is 20Vdc at 30Vdc.

Note: The door entry station can be powered by PoE+ or PoE Ethernet (with some restrictions)

Your device is delivered from the factory in PoE / PoE+ configuration, however in some cases it may be necessary to block it in a PoE configuration alone (distribution of the power of the Switch on several gatekeepers / poor power management of the Switch / ...).

In this case with the device not powered and with a small non-conductive clamp, remove the strap indicated in red on the photo below



### IP network connection (ETH0 / ETH1)

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

2 Available Ethernet port (1 PoE or PoE+ and 1 non PoE compatible)

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

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

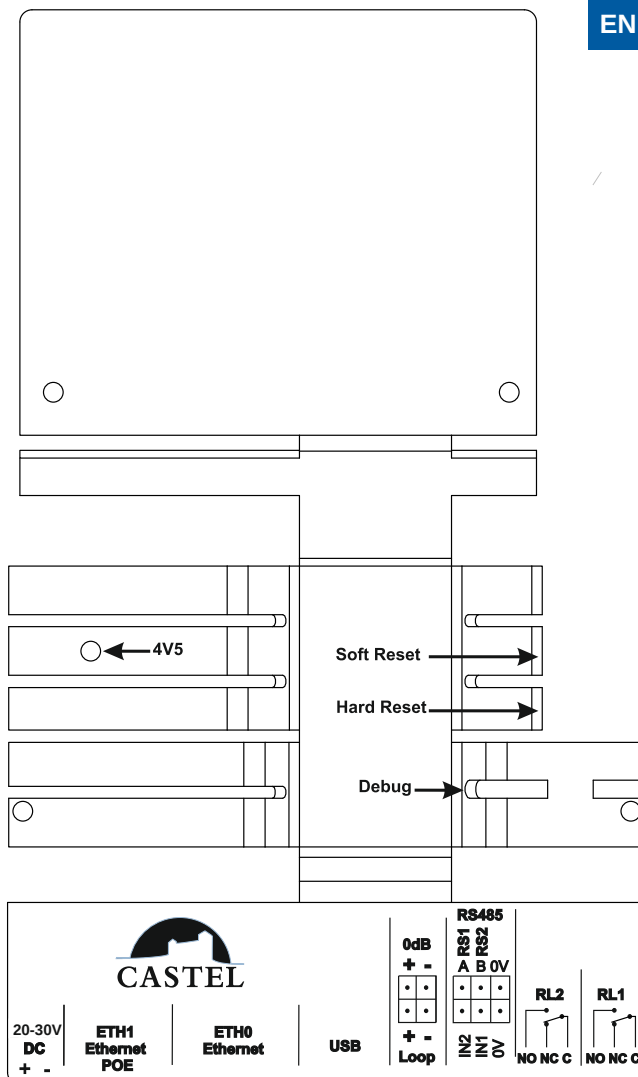
+: hot spot

-: cold point

0V: GND

### Magnetic Loop Loop Output Connection (Loop)

A Loop output allows the connection of the magnetic induction loop.



### Connection to the VDIP RS485 bus Configurable with CASTELSuite

The device is connected to the VDIP RS485 devices (VD4S réf 110.1000, VD8EI réf 110.1100, VDLECT réf 110.1200) via a RS485 bus line (bus wiring: several devices can be installed on one bus line).

The bus connection between the peripherals and the module is made by points RS1 and RS2 (via a twisted pair) and the ground. Establish the point-to-point connection by following the order of the signals.

The maximum length of the bus is 1 km. A 120Ω resistor needs to be fitted (provided with the RS485 device) between points RS1 and RS2 at each end of the bus.

### Input connection (IN1 / IN2 / 0V)

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

The contact can be deported up to 1Km.

### 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 use one of these relay outputs to control an AC or DC strike, wire a non-polarized 58V diode in parallel to the dry contact between C and NO or C and NC depending on use (diode supplied).

### Protection against electrostatic discharges

Connect the intercom to earth using the yellow lug supplied in the bag, then connect it to the fixing located next to the microphone.





## INSTALLATION

FR

### Flush mounting

Create a recess 271mm high, 143 mm wide and 61 mm deep in the support.

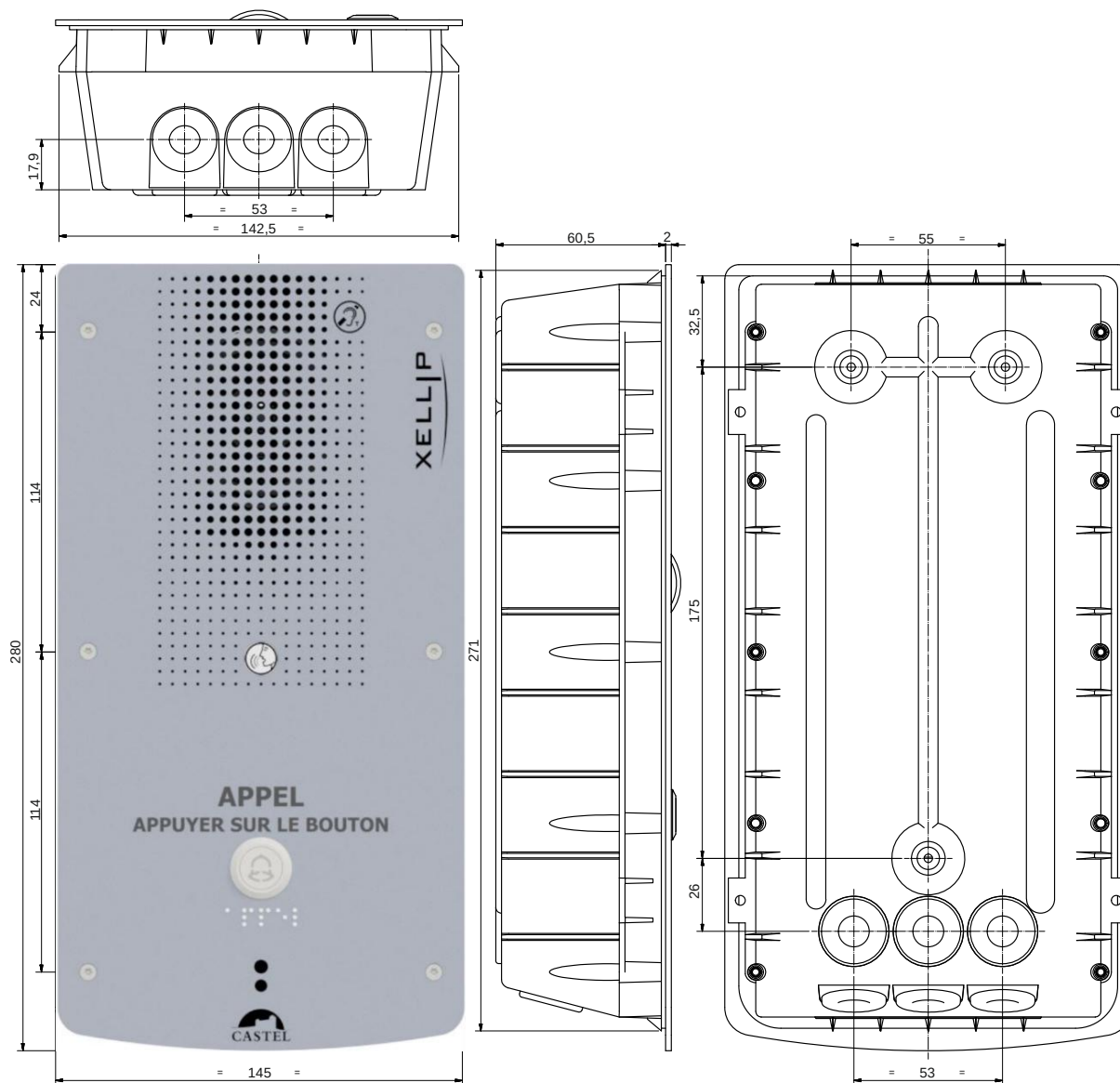
Mount the base in the recess then connect the entry station.

Attach the front panel with the 6 FX test screws (TORX) M3 x 10.

EN



Do not embed the bottom too deeply because when the front panel is fitted, the front panel's seal would no longer be in contact with it. This would cause the seal to break.



### Mounting on plasterboard wall

Create a recess 266mm high, 143 mm wide in the wall.

Mount the clamping kit (Option ref. 590.9600) on the entry station base.



Set the entry station base in the recess using the clamps then connect the entry station.

Attach the front panel with the 6 FX test screws (TORX) M3-10.

## Surface mounting

Fit the flush-mounted bottom onto the frame (Option ref. 590.9220) using 4 screws CZ M3 x 6.

Attach the assembly (bottom + frame) on support by three screws of diameter 3 to 3.5 max.

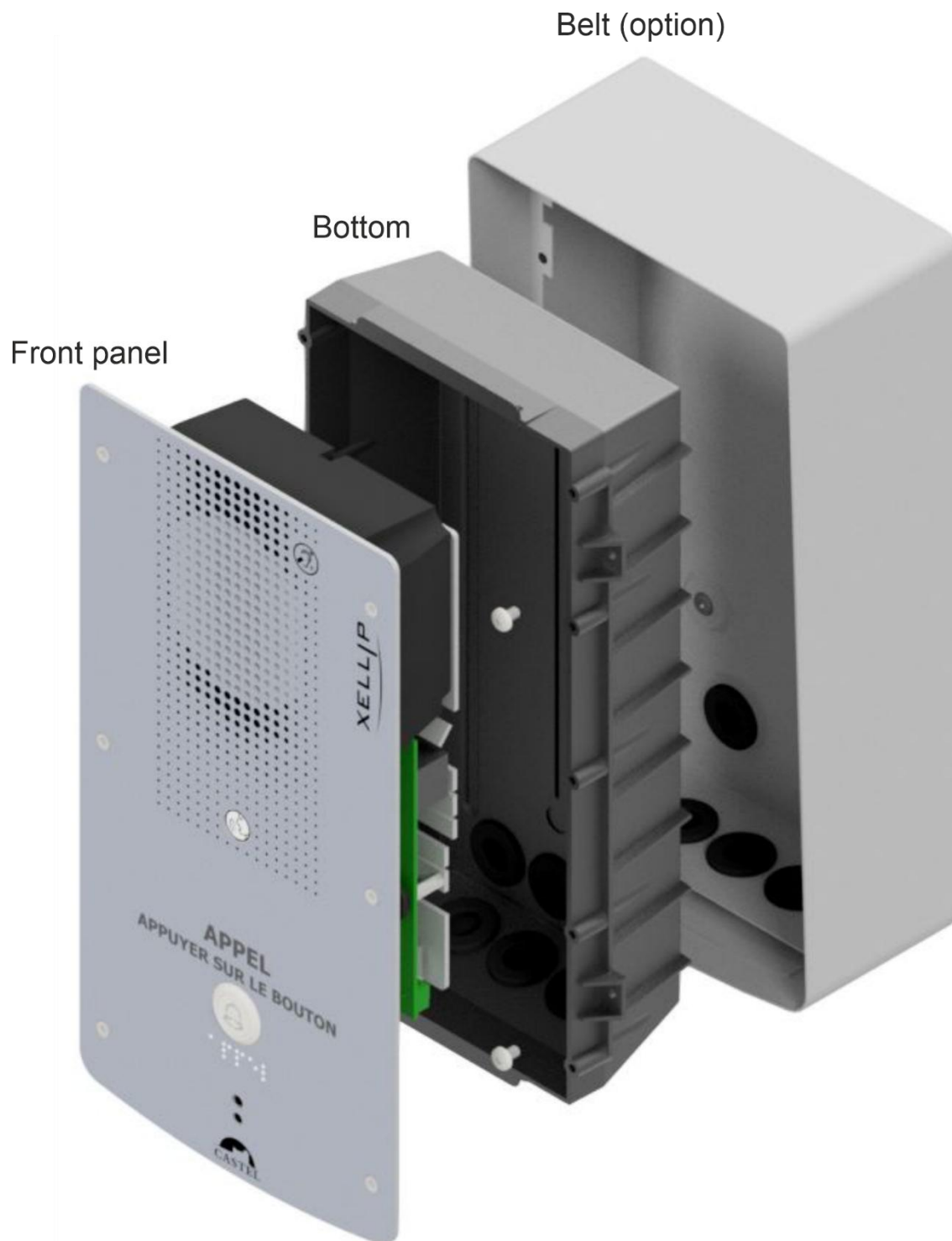
Connect the entry station.

Attach the front panel with the 6 FX test screws (TORX) M3 x 10.

To ensure your door entry system is properly sealed, it is necessary that the front panel, once fitted, presses against the entire sealing gasket located between the bottom and the front panel.

FR

EN



## Mounting the cap option

Stainless steel 316L cap. Dimensions: 275 x 147 x 27 mm

Flush mount the bottom.

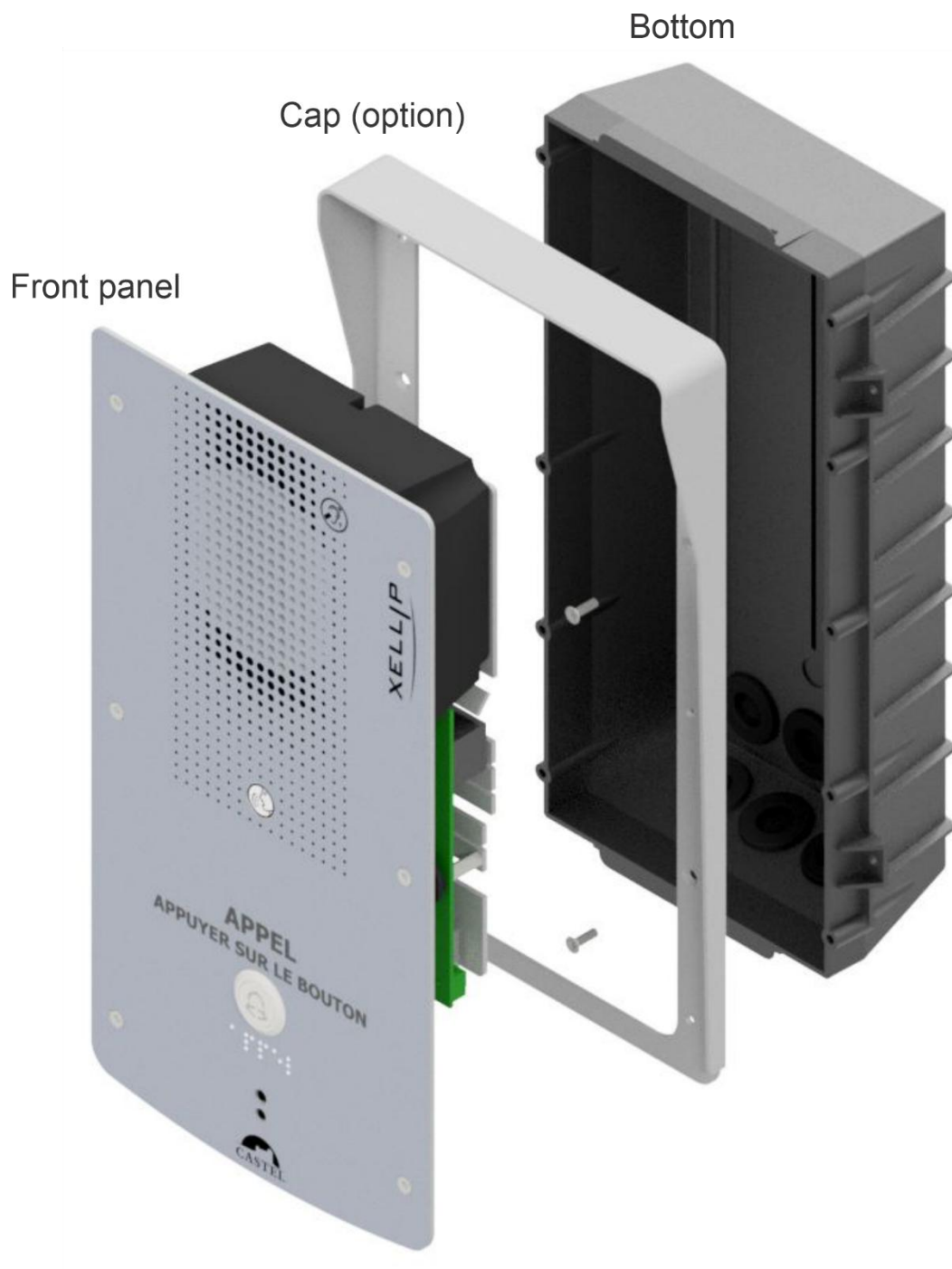
Attach the cap (Option ref. 590.9400) on the flush-mounted bottom using 4 screws FX (TORX) M3 x 10.

Connect the entry station.

Attach the front panel with the 6 FX test screws (TORX) M3 x 10.

FR

EN



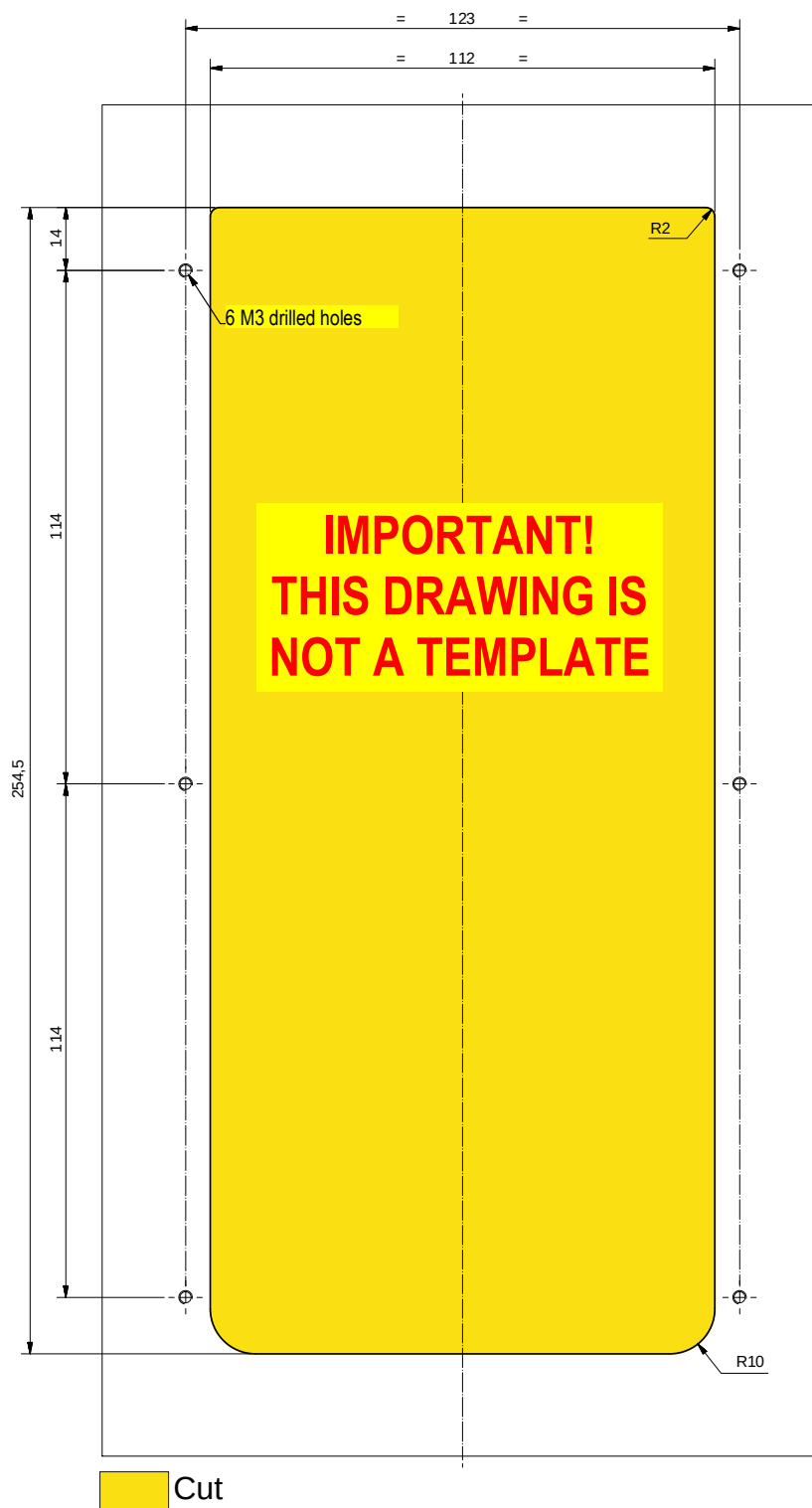
## Mounting on a post

Machine the opening on the post using the drawing below.

Connect the entry station.

Attach the front panel on the post with the 6 FX test screws (TORX) M3 x 10.

**IMPORTANT! The entry station is mounted without a base, the post must be watertight (IP 65).**



## USE

FR

### Station IP address

EN

The workstation is delivered with DHCP by default. If there is no DHCP server, the workstation receives 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 modifying the workstation configuration.

The IP address of the workstation can be found using :

- CastellIPSearch software
- CastelServeur software
- Any ONVIF discovery software

If it is not possible to discover the station's IP address :

In factory configuration, the set will state its IP address when the 1st programmable button is pressed.

The terminal also states its IP address when the "Soft Reset" push-button on the electronic board is pressed briefly.

If the "Soft Reset" button is pressed and held for more than 3 seconds, the telephone sets its IP address to 192.168.49.251.

### Station reset

When the "Soft Reset" button is pressed and held for more than 20 seconds, the terminal is restarted and the parameters are reset to the factory configuration.

Pressing the "Hard Reset" button only restarts the terminal immediately.

### Access to the workstation Web server

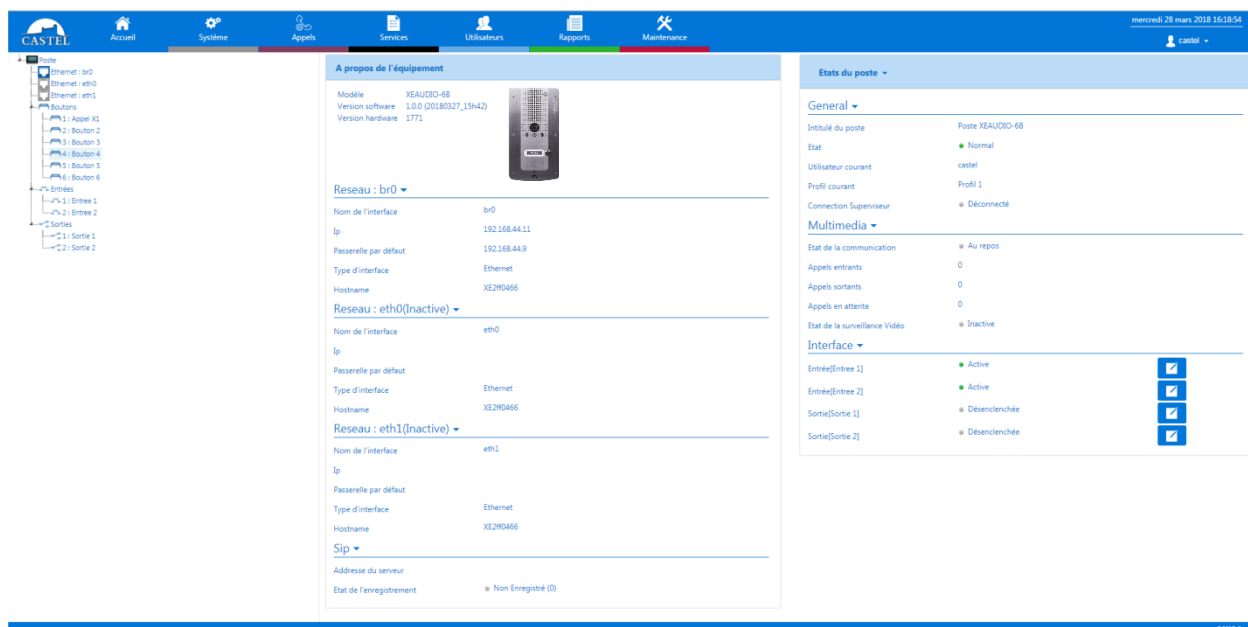
You can access the workstation's web server from a browser such as Chrome, Edge or Firefox.

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

There are 2 possible situations:

- Either your workstation is in factory configuration, and a wizard must be completed before any other operation.
- Or your workstation is already configured. Please enter the login and password 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.



## Wizard displayed on the web pages when the system is commissioned for the first time

FR

When the system is commissioned for the first time, a wizard will prompt you to define certain cybersecurity rules.

EN

Creating a new account

Reset

General conditions



### Welcome

As your workstation leaves the factory, you must choose which security policy you wish to implement. This policy can be changed later in the workstation's system settings.

For security reasons it is recommended to choose at least a moderate security policy

You must create a first administrator account.

It is advisable to make a backup at the end of the complete configuration of the workstation to be able to restore it if the administrator password is lost.

☐ I have read and accept the general conditions

Next

Creating a new account

Reset

Security policy (1/2)

Low

Moderate

High

Personalized

Password complexity

|                                                    | 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      |

Previous

Next

Creating a new account

Reset

Security policy (2/2)

Low

Moderate

High

Personalized

Firewall and services configuration

Activate the firewall

☐

Web service

☐

HTTP

☐

CastelSuite and inter-equipment connection

☐

Enable connection to CastelSuite and inter-device connections

☐

Previous

Next

Creating a new account

Reset

Account

castel

\*\*\*\*\*

Confirm password

✗ Minimum number of characters : 10

✗ Minimum number of capital letters : 1

✗ Minimum number of digits : 1

✗ Minimum number of special characters : 1

✗ Confirm password

!

 Any loss of password will result in a factory reset!

Previous

Next

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

- On the level of complexity of the passwords which will be applied to each account creation and in particular for the administrator account.
- On 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 must only be cleaned using a mild cleaning product (water or soapy water) that is non-abrasive, non-foaming and above all free from any type of solvent or alcohol.

For regular maintenance, only use water, without detergent.

Jet cleaning must be prohibited, as well as use of abrasive sponges and cloths with aggressive surfaces.



## FUNCTIONS

FR

EN

The station is designed to communicate with all the devices from 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 devices from the Castel digital and analog intercom range. This type of communication requires the use of an additional M-HYB-IP gateway.

### General functions of the entry station

- Establish audio/video communication in accordance with the SIP standard:
  - ↳ Point to point
  - ↳ By registering on a SIP server. Multiple SIP accounts can be defined, each with up to 2 backup servers. With support for UDP, TCP and TLS network transport protocols.
- Management of audio and video communications (depending on version).
  - ↳ Possibility of defining the extension's priority level
  - ↳ Possibility of defining the call and communication timeout
  - ↳ With or without automatic pick-up, with or without delay
  - ↳ Secret mode can be activated on automatic pick-up
- Date and time can be set manually or via an NTP server. The telephone can also be used as an NTP server.
- Native interfacing with Synchronic access control. Allows you to set the parameters required for proper operation: certificate management, access configuration, etc.

### Security & network functions

- Configurable network interface with a choice of 1 or 2 separate or bridged interfaces and the option of adjusting the communication speed (10/100/1000Mbit/s)
- VLAN support
- Support for Spanning Tree Protocol to manage network loops
- Possibility of enabling secure Ethernet connections via the 802.1X protocol (RADIUS). Authentication protocols supported: EAP-TLS, EAP-TTLS, PEAP and EAP-MD5.
- Definition of a security policy and implementation of a firewall resulting in :
  - ↳ Definition of password complexity
  - ↳ Restrictions on the use of services (in particular the closing of unused ports) with the possibility of defining personalised firewall rules
  - ↳ The ability to restrict access to services to equipment by IP address range

### Audio interface functions

- Configure the audio algorithm to adjust Acoustic Echo Cancellation (AEC), Ambient Noise Reduction (NR) and Acoustic Echo Suppression (AES).
- Configure speaker volume, microphone volume and hearing loop volume
- Configure ringtones and tones
- Configure noise detection parameters. Used, 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. Used, for example, to activate a relay during a call.
- Switch to simplex on receipt of a DTMF command (from the remote station).
  - ↳ "\*" switches to listening simplex
  - ↳ "#" switches to speech simplex
  - ↳ "0" is used to return to standard operation

### Programmable button functions

Each button can be programmed and is used to:

- Call 1 to 10 stations simultaneously or with timeout
- Control the local relay, the station relay in communication or send a DTMF code
- End a call
- Perform a list of advanced actions

### Digital input interface functions

- Configuring the type of input: STATUS or COUNTER
- Configuring the input active state: open or closed contact
- Configuring a delay for taking into account a change of state (anti-rebound function)
- Configuring the counter threshold
- Inhibit the input

## Output interface functions

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

## Logical input functions (or flags)

The logical inputs enable two functionalities in particular:

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

The configuration of the logical inputs requires the use of the CastelServeur software.

## Configuring relations

**The Web server is where automatic controls, also called relations, are configured**

There are two types of relations:

- Scheduled: used to trigger actions at identified time slots. There are three levels of priority for a schedule relation (high, medium and low).
- Logical:
  - ↳ Logical condition: used to trigger actions at certain status conditions (active, inactive, etc.). A logical relation can integrate several conditions by operators such as AND, OR, NOT, XOR. Likewise, a logical relation can trigger several actions.
  - ↳ Digital condition (Counting): used to perform actions by comparing the value of a counter with different thresholds. It is also possible to add or subtract counter values and compare the result obtained.

## User configuration

The workstation server allows you to create, modify or delete users.

There are several types of user:

- Web: users authorised to connect and use the workstation's configuration web pages
- RTSP: users who can use the workstation's audio/video streaming service
- ONVIF: users who can use the workstation's ONVIF service.

A username and password is required for each user.

For web users, it is also possible to:

- Define the display language when the user is connected.
- Associated rights

## Profile configuration

Station operating profiles can be created, modified or deleted. Each profile specifies a station priority, a configuration of function buttons and access rights to the station.

The station can operate with a unique profile or with different profiles according to time slots.

## ONVIF (Open Network Video Interface Forum) function

The station is compatible with the ONVIF protocol.

From web pages, it is possible to activate or deactivate ONVIF discovery.

It is possible to configure the scopes.

## RTSP (Real Time Streaming Protocol) function

The station integrates an RTSP server allowing an external RTSP client to retrieve the audio and/or video stream from the station.

An authentication mechanism can be activated to secure access to the stream.

It is possible to define the audio parameters for the stream.

## SNMP (Simple Network Management Protocol) function

The station integrates an SNMP agent that can respond to SNMP queries and send notifications (TRAPS) to an SNMP manager.

From web pages, it is possible to:

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

SNMPv1 and SNMPv2c versions are supported.

## ASCII notification function

The station incorporates a notification mechanism through ASCII strings.

From web pages, it is possible to:

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

## Self-test function

The station has several tests to validate its operation:

- HP/MIC self-test: can remotely test the right operation of the speaker and microphone. From the 'advanced parameters' page, the levels of this test can be adapted according to the installation environment. This test can be activated from the web server or by an SNMP command. The result of the test can be consulted from the web server history and by an SNMP notification.
- Mechanical button self-test: the detection of a locked mechanical button (contact made for more than 20 s) is signalled by an SNMP notification and an event is signalled in the web server history.

## Event feed function

This function allows you to view all the events that have occurred on the substation. They are listed with the date and time of the event concerned and the associated information.

## Call log function

The call log is a simple way of viewing the history of communication events: calls received, calls made, calls established and call transfers or diversions.

## Security function

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

## Backup and recovery of system parameters

It is possible to back up or restore all the workstation's parameters (configuration, profiles, relationships, directory, etc.).

You can reset the terminal to its factory configuration by pressing the reset button for 10 seconds when the terminal starts up.

## Station update

You can update your workstation by sending a file containing the new software version.

The machine then reboots automatically to apply the update. The update does not change any user settings.

## Backup on power outage

When a power failure occurs, the station can save the following information:

- Counter values
- History
- The backed-up events (these events are defined from CastelServeur)
- Interface states

## TECHNICAL CHARACTERISTICS

FR

EN

### Compliance with european directives

- 2001/95/EC: Safety
- 2014/30/UE: EMC
- 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

- IK07 vandal resistant design according to EN 62262
- Degree of protection IP65 as per EN 60529
- 316L stainless steel front panel
- Flush ABS base with wall mounting
- Dimensions: H 280 x L 145 x P 63 mm
- Weight: 1,4kg

### General electric characteristics

- Operating temperature: -20° to +50°C.
- Storage temperature -20° to +70°C.
- Relative humidity: <90%, without condensation.
- External power :
  - ↳ 24VDC (20V à 30V) 30W max
- Power PoE IEEE 802.3af 12,9W max

### Buttons

- Acquisition speed 5Hz (200ms)

### Inputs

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

### Outputs

- 2 potential-free relay outputs
- Relay cutoff power 42.4VAC/60 VDC/5 A/150VA
- The maximum frequency is 5Hz (minimum switching time: 200ms)

### Audio

Maximum sound power:

- If powered by PoE: 1W
  - ↳ LAeq 78.5dB @1m (pink noise)
  - ↳ LAeq 87dB @1m (1000Hz sine wave)
- If powered by PoE+: 6W
  - ↳ LAeq 85dB @1m (pink noise)
  - ↳ LAeq 90dB @1m (1000Hz sinusoid)
- If external power supply: 10W
  - ↳ LAeq 85,7dB @1m (pink noise)
  - ↳ LAeq 91dB @1m (1000Hz sinusoid)

Sampling frequency: 16KHz

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

### DTMF

- RFC-2833
- SIP INFO

### Security & Networking

- PoE compliant 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 the ability to list active services & ports
  - ↳ Adaptive security policy
  - ↳ IP address restriction

### Use

For optimum communication, the distance between the intercom and the caller should not exceed 1m.



#### Environmental protection:

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