PRESENTATION

Références produits : 590.1060 (XE AUDIO 1B CLAV BLE) - 590.1160 (XE VIDEO 1B CLAV BLE) - 590.6400 (XE AUDIO 1B BLE) - 590.6900 (XE VIDEO 1B BLE) – 590.5500 (XE AUDIO 2B BLE) - 590.6000 (XE VIDEO 2B BLE) – 590.6930 (XE VIDEO 4B BLE) - 590.7400 (XE PAD AUDIO BLE) - 590.7900 (XE PAD VIDEO BLE) – 590.7410 (XE PAD AUDIO CLAV BLE) - 590.7910 (XE PAD VIDEO CLAV BLE) – 591.6000 (XE VIDEO 2B BLE DO) – 591.6900 (XE VIDEO 1B BLE DO) – 591.7900 (XE PAD VIDEO BLE DO)

Votre équipement d'interphonie SIP propose les fonctionnalités suivantes (selon les versions) :

- 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 chaines ASCII
  - ↘ Lecture de QRCode et de codes-barres permettant des automatismes
- 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 (selon les versions) :

- Caméra grand-angle Full HD, protégée par un hublot démontable
- Ecran TFT 2.8 pouces permettant de visualiser et d'appeler des noms dans un annuaire
- Clavier numérique pour numérotation et composition d'un code d'accès
- Lecteur de contrôle d'accès intégré compatible avec les normes ISO14443 type A & 3B et Bluetooth permettant :
  - ↘ Soit un contrôle d'accès localisé au poste
  - ↘ Soit un contrôle d'accès supervisé à travers la solution CastelAccès
  - ↘ Soit un contrôle d'accès supervisé à travers la solution Synchronic
  - ↘ Soit un contrôle d'accès tiers lorsque la sortie bornier de la carte lecteur est raccordée à cet effet
- 1 à 2 boutons d'appel programmables pour configurer des actions au choix
- 6 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.
- Conforme à la « loi accessibilité aux personnes avec handicap » : poste équipé de pictogrammes, de LED de couleur, de synthèses vocales, d'une boucle d'induction magnétique

FR

EN

VERSIONS

- Version 1 BP, 2 BP + lecteur bluetooth multi-technologies : Audio seul
- Version 1 BP, 2 BP + lecteur bluetooth multi-technologies : Audio et Vidéo
- Version DO 1 BP, 2 BP + lecteur bluetooth multi-technologies : Audio et Vidéo, présence d'un contact de détection d'ouverture
- Version Défilement de nom + lecteur bluetooth multi-technologies : Audio seul
- Version Défilement de nom + lecteur bluetooth multi-technologies : Audio et Vidéo
- Version DO Défilement de nom + lecteur bluetooth multi-technologies : Audio et Vidéo, présence d'un contact de détection d'ouverture
- Version Défilement de nom + clavier + lecteur bluetooth multi-technologies : Audio seul
- Version Défilement de nom + clavier + lecteur bluetooth multi-technologies : Audio et Vidéo

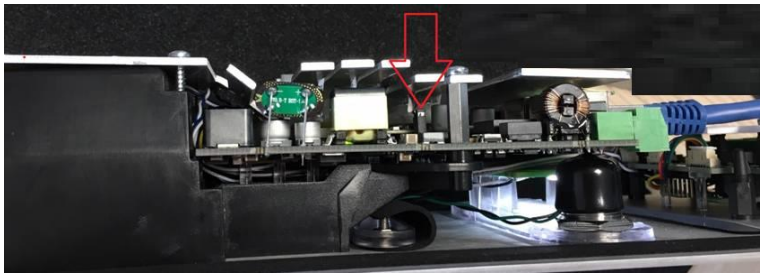
OPTIONS

- Référence 590.9320 : Ceinture pour modèles sans clavier numérique
- Référence 590.9500 : Casquette pour modèles sans clavier numérique
- Référence 590.9600 : Kit griffes pour modèles sans clavier numérique (Montage sur placoplâtre)
- Référence 590.9100 : Fond montage saillie pour modèles avec clavier numérique
- Référence 910.0205 : KIT PROG ARC13.56MHz+BLUETOOTH (nécessaire pour une gestion évoluée)
- Référence 910.0206 : Crédit Badge Virtuel STid Mobile ID
- Référence 120.9500 : Enroleur USB Bluetooth de table

RACCORDEMENT

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



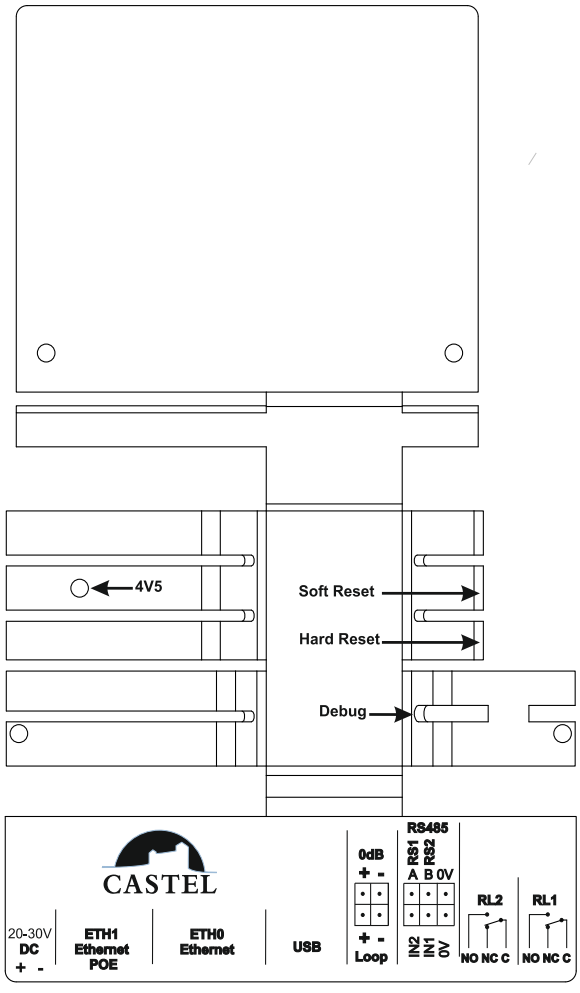
Raccordement au réseau IP (ETH0 / ETH1)

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



FR

EN

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)

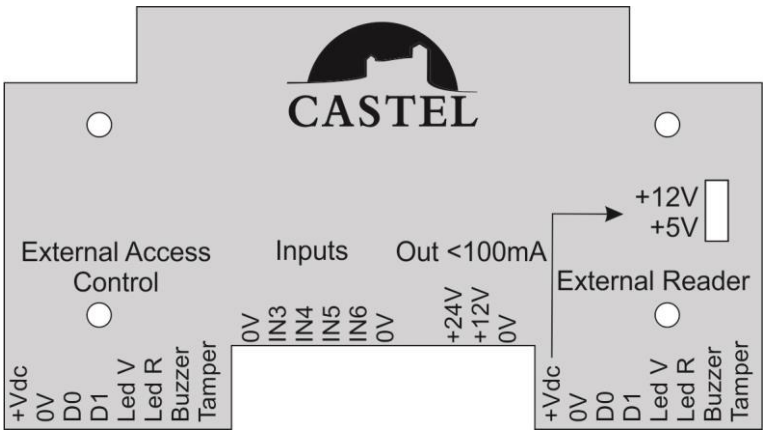
Deux entrées TOR permettent le raccordement d'un contact sec (ne pas appliquer de tension). Pour être activée, l'entrée doit être tirée à la masse.
Le contact peut être déporté jusqu'à 1Km.

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 fournie (Montée sur la fixation du micro).



Raccordement des entrées 3 à 6 (Inputs) *Applicable à partir de la version software 1.5.0*

Quatre entrées TOR (IN3 / IN4 / IN5 / IN6) permettent le raccordement d'un contact sec (ne pas appliquer de tension). Pour être activée, l'entrée doit être tirée à la masse (0V).
Le contact peut être déporté jusqu'à 1Km.

Source d'alimentation 12V ou 24V pour accessoires (Out <100mA)

Fonction uniquement disponible lorsque le portier est alimenté en PoE+ ou par une alimentation externe, il fourni une alimentation pour alimenter des accessoires externe comme par exemple un BP de sortie, un radar, un voyant dans la limite de 24V/50mA max ou 12V/100mA max.

Raccordement du lecteur externe (External Reader)

Le lecteur, clavier à code ou lecteur équipé d'un clavier raccordé peut être de type Wiegand (D0 & D1).
Les formats compatibles sont Wiegand 26, 32, 34, 37, 44, 56 et 58 bits
Deux sorties collecteur ouvert permettent de commander les LED Rouge (LED R) et Verte (LED V) du lecteur ou clavier à code raccordé.
Lorsque le portier est alimenté en PoE+ ou par une alimentation externe, il peut alimenter le lecteur externe (+VDC / 0V) dans la limite de 5V/100mA ou 12V/100mA (et jusqu'à 200mA si la source d'alimentation 12V accessoires n'est pas utilisée). Pour tout lecteur ayant une consommation supérieur, prévoir une alimentation externe.
Le raccordement se fait par liaison fil à fil, voir la fiche technique du lecteur raccordé.

Raccordement du système de contrôle d'accès externe (External Access Control)

Le lecteur intégré au portier est muni d'un connecteur 8 points permettant son raccordement au système de contrôle d'accès client. Dans ce cas d'utilisation, le lecteur n'est plus géré par le portier CASTEL et doit être alimenté par le système de contrôle d'accès externe.
La distance maximale entre le lecteur et le système de contrôle d'accès est de 100m max avec du câble de type 6/10.
Relier une extrémité de l'écran du câble à la masse.
L'alimentation requise (+VDC / 0V)

- Alimentation 9 à 15VDC
- Consommation: 150mA/12V

L'interface est de type Wiegand (D0 & D1) 56 bits.
Deux entrées permettent de commander les LED Rouge (LED R) et Verte (LED V)
Une entrée « Buzzer » permet de commander le buzzer du lecteur
Une sortie « Tamper » permet de signaler l'arrachement, ne pas raccorder car non disponible.

FR

EN

Raccordement du contact de détection d'ouverture (Version DO)

DETECTION CONNECTEE AU BOITIER

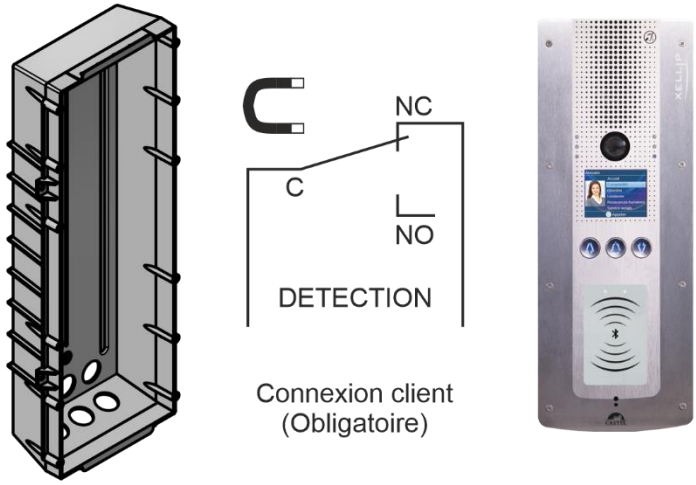
- Evénement de remontée d'ouverture
- Commande du relais à paramétrer

Fond arrière	Détection	Entrée IN1
Ouvert	NC/C	Activée
Fermé	NO/C	Désactivée

NC : Normalement Clos
NO : Normalement Ouvert
C : Commun

DETECTION DIRECTE

- Pas de remontée d'ouverture sur le portier
- Commutation du relais magnétique à l'ouverture
- Utilisation directe du contact 20VDC/0,5A



Fond arrière	Détection
Ouvert	NC/C
Fermé	NO/C

NC : Normalement Clos
NO : Normalement Ouvert
C : Commun

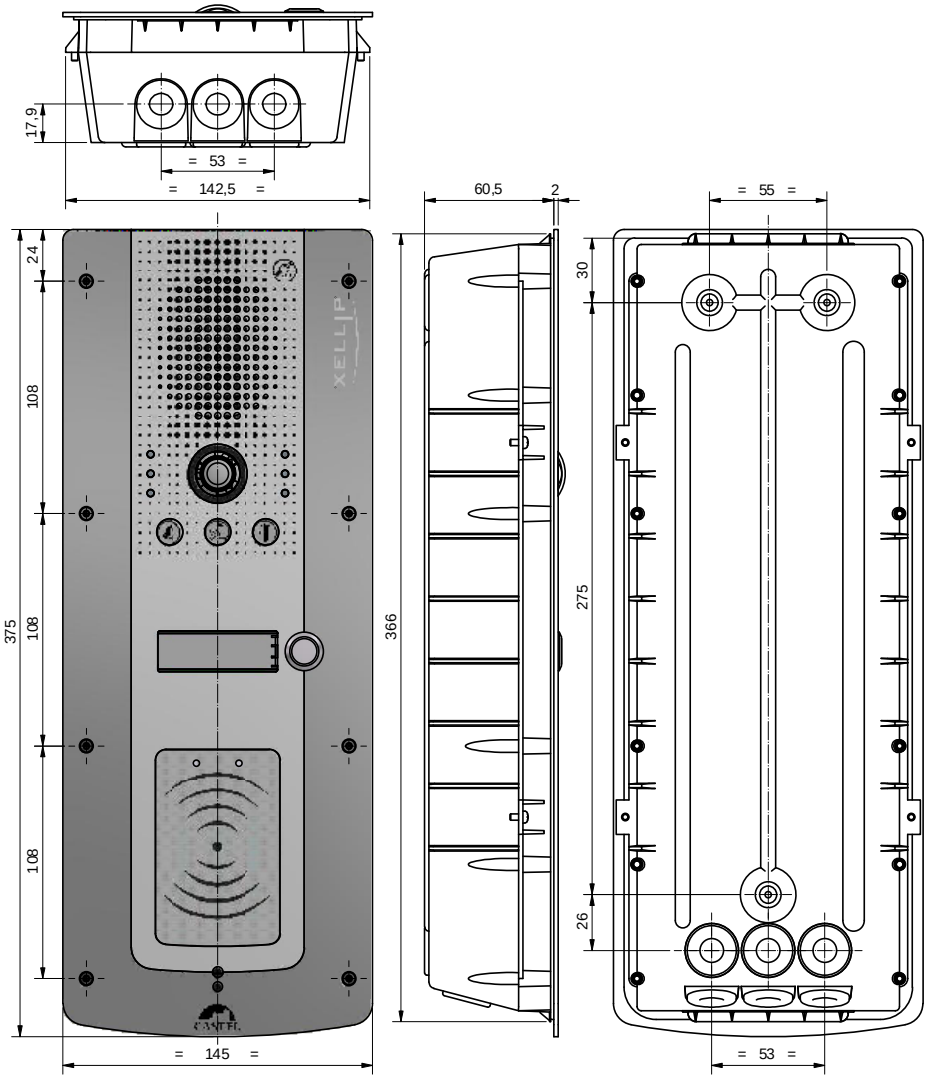
FR

EN

INSTALLATION

Montage en encastrement des modèles sans clavier nurérique

Faire une réservation hauteur 367mm, largeur 143mm et profondeur 65mm dans le support.
Enduire le fond de la réservation d'au moins 10mm de ciment frais.
Introduire le fond du portier dans la réservation et le pousser. Laisser le fond dépasser de 2mm.
Laisser sécher le ciment au moins 24H, puis raccorder le portier.
Fixer la face avant avec les 8 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.



Montage sur cloison en Placoplatre

Faire une réservation hauteur 361mm, 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 8 vis FX (TORX) à téton M3 x 10.

FR

EN

Montage en saillie des modèles sans clavier numérique

Fixer le fond encastrable sur la ceinture (Option réf. 590.9320) 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 8 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 des modèles sans clavier numérique

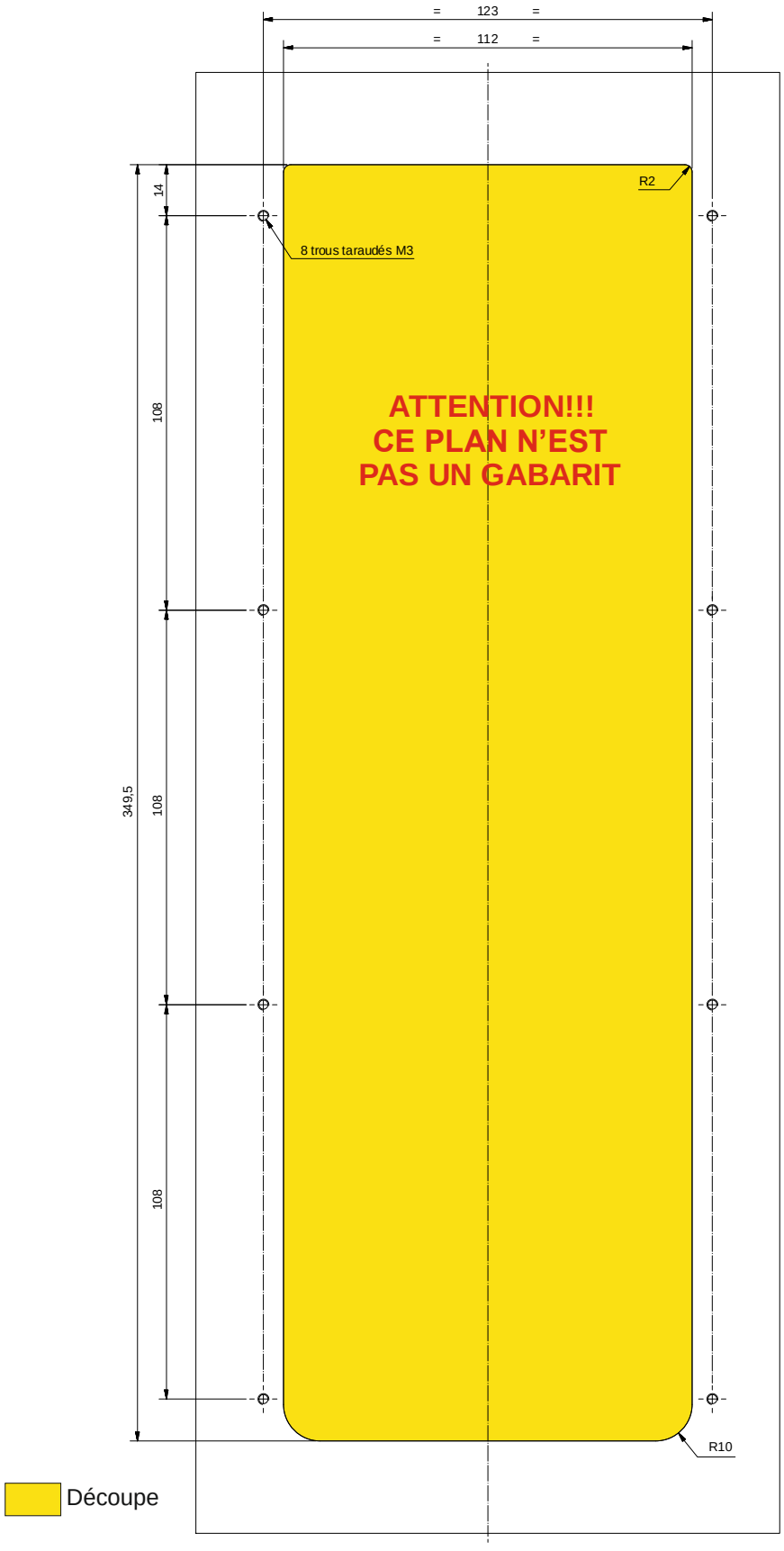
Casquette en inox 316L. Dimensions : H 370,5 x L 149 x P 26 mm
Encastrer le fond.
Fixer la casquette (Option réf. 590.9500) sur le fond encastrable à l'aide des 4 vis FX (TORX) M3 x 10.
Raccorder le portier.
Fixer la face avant avec les 8 vis FX (TORX) à téton M3 x 10.
Pour garantir à votre portier une bonne étanchéité, il est nécessaire que la face avant une fois montée, appuie sur la totalité du joint d'étanchéité situé entre la casquette et la face avant et entre la casquette et le fond.

FR

EN

Montage sur potelet des modèles sans clavier numérique

Usiner l'ouverture sur le potelet suivant le plan ci-après.
Raccorder le portier.
Fixer la face avant sur le potelet avec les 8 vis FX (TORX) à téton M3 x 10.
ATTENTION!!! Le portier étant monté sans son fond, le potelet doit impérativement être étanche (IP 65).

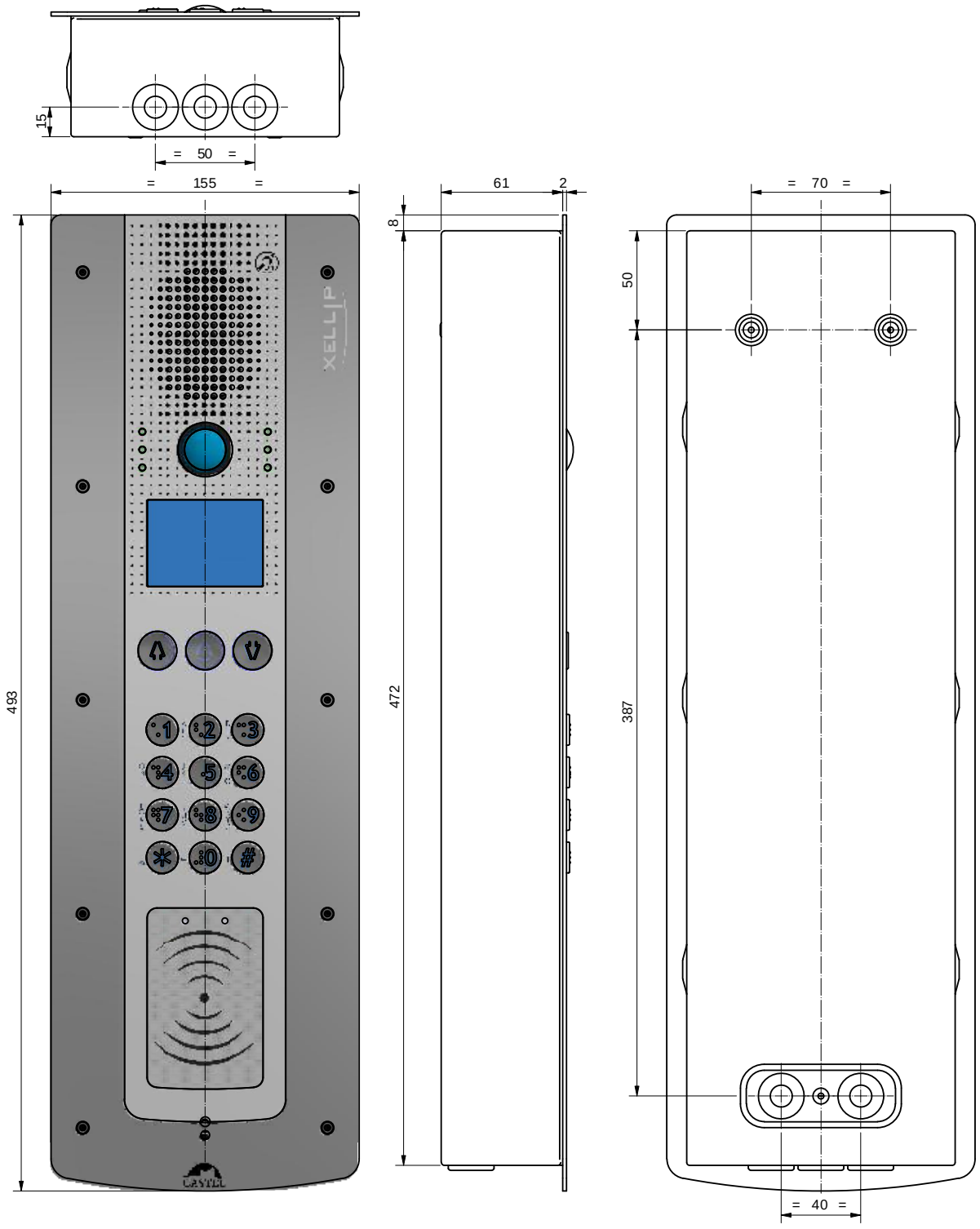


FR

EN

Montage en encastrement des modèles avec clavier numérique

Faire une réservation hauteur 477mm, largeur 144mm et profondeur 65mm dans le support.
Enduire le fond de la réservation d'au moins 10mm de ciment frais.
Introduire le fond du portier dans la réservation et le pousser. Laisser le fond dépasser de 2mm.
Laisser sécher le ciment au moins 24H, puis raccorder le portier.
Fixer la face avant avec les 10 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 en saillie des modèles avec clavier numérique

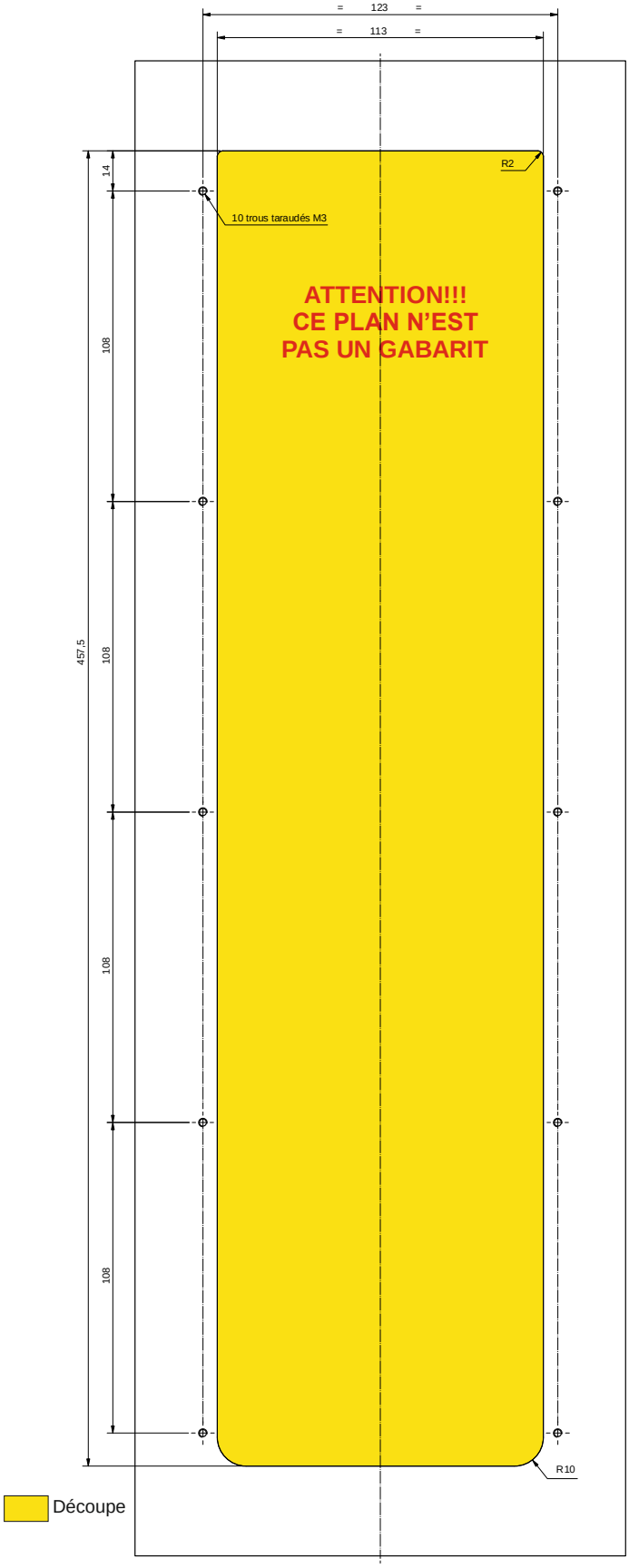
Fixer le fond saillie (Option 590.9100) sur son support.
Raccorder le portier.
Fixer la face avant avec les 10 vis FX (TORX) à téton M3 x 10.
Pour garantir à votre portier une bonne étanchéité, il est nécessaire que la face avant une fois montée, appuie sur la totalité du joint d'étanchéité situé entre le fond et la face avant.

FR

EN

Montage sur potelet des modèles avec claviers numérique

Usiner l'ouverture sur le potelet suivant le plan ci-après.
Raccorder le portier.
Fixer la face avant sur le potelet avec les 10 vis FX (TORX) à téton M3 x 10.
ATTENTION!!! Le portier étant monté sans son fond, le potelet doit impérativement être étanche (IP 65).



FR

EN

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 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 1er 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 » entraine un redémarrage du poste et la réinitialisation des paramètres en configuration usine.
Un appui sur le bouton « Hard Reset » entraine 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 tout 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.

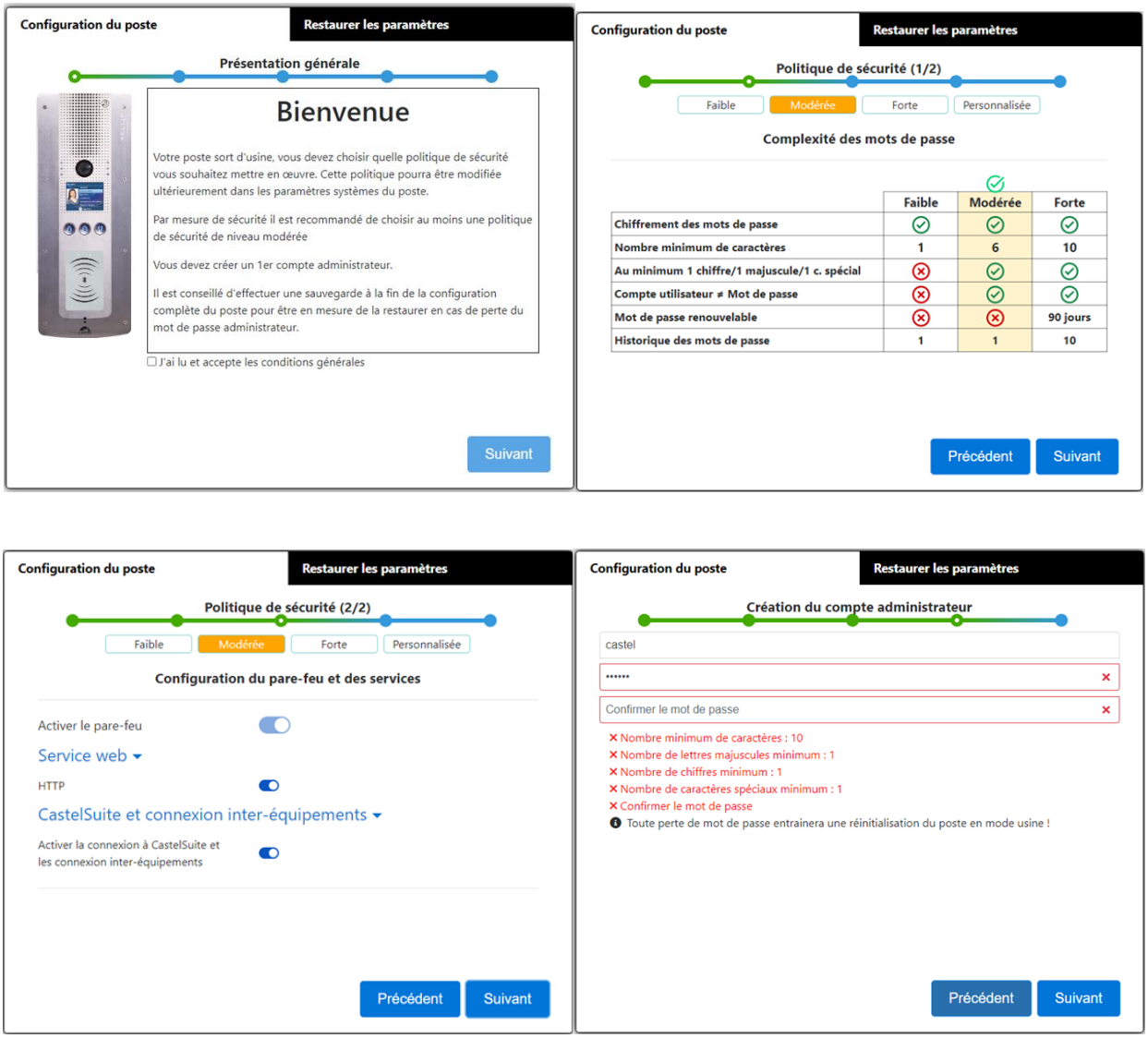
A noter : une aide en ligne est accessible à partir de tous les menus. Cette aide permet de s'informer sur les différentes fonctions du serveur Web.

FR

EN

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

A la 1ière mise en service, un wizard vous invite à définir certaines règles de cybersécurité.



En 1er 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

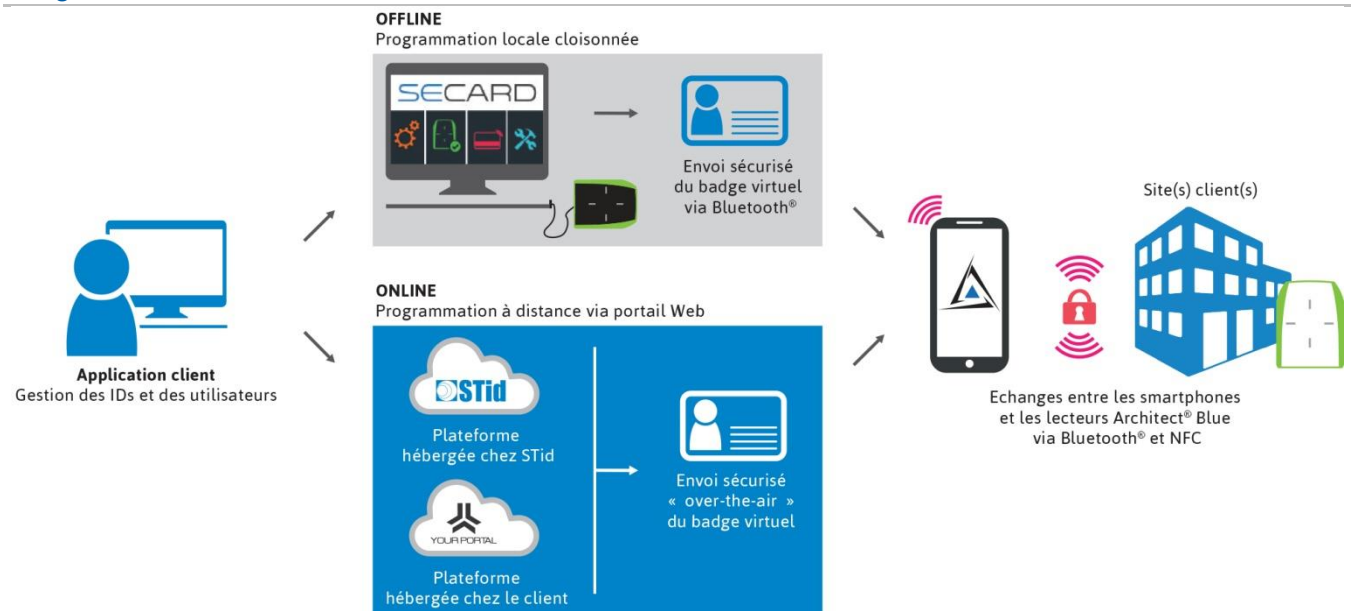
Le nettoyage de votre produit CASTEL doit être réalisé uniquement à l'aide d'un produit nettoyant doux (eau ou eau savonneuse), non abrasif, non moussant et surtout exempt de tout type de solvant ou alcool.
Pour l'entretien courant, utilisez uniquement de l'eau, sans détergent.
Le nettoyage au jet est à proscrire, ainsi que les éponges abrasives et tissus à surface agressive.

FR

EN

UTILISATION DE LA SOLUTION BLUETOOTH

Intégration de la solution



La solution d'identification sécurisée et conviviale STid Mobile ID® transfère le badge d'accès sur les Smartphones Android™ et iOS®, en complément ou remplacement de la carte RFID traditionnelle.
Elle inclut une application mobile gratuite, la dernière génération de lecteurs multi-technologies et des outils de configuration Offline et Online.

L'application Offline

- Permet de créer des badges virtuels localement, de la même manière que les badges classiques.
- Programmation cloisonnée 100% locale
- Maîtrise complète des paramètres de sécurité et de configuration

L'application Online

- Transmet un badge virtuel instantanément à un utilisateur distant, grâce à un serveur Web sécurisé (https)
- Echanges sécurisés de droits entre serveur et smartphone
- Gestion dynamique des droits : création, révocation et mise à jour à distance
- Données hébergées sur serveur STid, Portail Web sécurisé Https

Mode de contrôle d'accès Bluetooth

Mode Badge

Présentez votre smartphone devant le lecteur comme un badge classique.

Mode Tap Tap

Tapotez. Entrez ! Vous pouvez ouvrir une porte en tapotant deux fois votre smartphone dans votre poche pour une ouverture à proximité ou à distance.

Mode Remote

Pressez. Entrez ! Activez le mode télécommande pour contrôler vos points d'accès à distance.

Mode Mains-libres

Passez simplement devant le lecteur sans action de votre part.

FR

EN

Applications mobiles

STid Moblie ID

- L'application STid Mobile ID® est un portefeuille virtuel de badges d'accès. Elle peut recevoir et stocker un nombre illimité de badges. Chaque badge virtuel porte un identifiant sécurisé, programmé par le client/utilisateur ou prédéfini.
- STid Mobile ID® est téléchargeable sur les plateformes Google Play (Android) et App Store (iOS). 95% des Smartphones du marché fonctionnent avec l'un de ces 2 systèmes d'exploitation
- L'application STid Mobile ID® est gratuite. Un badge virtuel CSN gratuit - STid Mobile ID® - est directement stocké dans l'application avec un numéro unique attribué à l'installation.

STid Settings

- STid Settings est un portefeuille virtuel de badges de configuration permettant de les stocker dans votre smartphone et de paramétrer les lecteurs en toute simplicité
- STid Settings est téléchargeable sur les plateformes Google Play (Android) et App Store (iOS). 95% des smartphones du marché fonctionnent avec l'un de ces 2 systèmes d'exploitation
- L'application STid Settings est gratuite.

Badges Virtuels

Un badge virtuel est la dématérialisation de vos badges de contrôle d'accès au sein d'une application mobile. Votre badge virtuel porte un identifiant et se comporte comme un badge RFID
Il existe 3 types de badges d'accès adaptés à vos besoins :

CSN STid Mobile ID:

- Numéro unique fourni à l'installation
- Mode autorisé : mode badge
- Coût : gratuit, fourni avec l'application STid Mobile ID

CSN STid Mobile ID+:

- Numéro unique fourni à l'installation
- Mode autorisé : mode badge, Tap Tap , main libre.
- Coût : 1 crédit

Virtual Access Card

- ID privé
- Sécurité entièrement paramétrable
- Mode autorisé : mode badge, Tap Tap, main libre, remote.
- Coût : 5 crédits

Configuration du lecteur

Le lecteur est livré préconfiguré usine pour faire de la lecture de numéro de série des badges Mifare Classic, Mifare Plus, Mifare UltraLight, Mifare DESFire, Blue, CPS3 et ISO14443B-3B.
Trois badges de configurations (SCB) fournis avec le portier permettent d'activer les modes de contrôle d'accès bluetooth :

- Mode Badge + Contact
- Mode Badge + Contact + Tap-Tap
- Mode Badge + Contact + Mains-libres.

L'ensemble des paramètres configurable du lecteur sont accessible avec le kit de programmation KIT PROG ARC13.56MHz+BLUETOOTH (réf 910.0205)
Si le SCB est compatible avec le firmware du lecteur, le buzzer retentit 5 fois.
Si le SCB n'est pas compatible avec le firmware du lecteur, le buzzer est activé 1s.

FR

EN

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/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 entrainant :
  - ↘ 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 de l'interface vidéo

- Configurer les paramètres vidéos de communication : port RTP, codecs vidéos (H264 / H263 & H263+)
- Configurer la résolution (QCIF / QVGA / CIF / VGA / HD / Full HD)
- Possibilité de gérer la bande passante en communication
- Possibilité d'ajuster les réglages de la caméra

Fonctions des boutons programmables

Chaque 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 de la touche « Appel défilement »

- Cette touche est la touche principale des postes à défilement de noms.
- De manière générale, elle permet de valider l'action en cours.
- Lorsque le portier est au repos, cette touche est programmable, elle permet de de faire un appel de 1 à 10 postes simultanés ou temporisés et d'afficher un menu d'aide à l'utilisation du portier.

Fonctions du lecteur de badge

- Configurer le type de badge.
- Inhiber le lecteur
- Réaliser un contrôle d'accès :
  - ↘ Soit localisé au poste
  - ↘ Soit supervisé à travers la solution CastelAccès
  - ↘ Soit supervisé à travers la solution Synchronic

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 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.

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 de l'annuaire

Il est possible de créer, modifier ou supprimer des entrées dans l'annuaire du poste.
Il est possible de créer des entrées pour des appels simples ou des appels multiples

Configuration de l'accès local

Il est possible de configurer un contrôle d'accès simplifié directement sur le poste :

- Programmation de 1 à 45000 codes d'accès de 1 à 20 chiffres.
- Programmation d'action(s) associée(s) à l'autorisation et au refus de l'accès par relation logique.
- Prise en compte de 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 chaines 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 QRCode et codes-barres

Le poste permet la lecture de QRCode et de codes-barres lorsque le service RTSP vidéo n'est pas activé.
Il est possible d'activer ou non cette fonctionnalité en fonction du profil.
Les formats des codes-barres reconnus sont les suivants : EAN-8, EAN-13 (et ses dérivés ISBN-10, ISBN-13...), I2/5, Code-39 et Code-128.
Il est possible de déclencher des automatismes sur détection d'un QRCode ou d'un code barre dans les relations.

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.

FR

EN

Fonction Fil de l'eau des événements

Le fil de l'eau permet de visualiser tous les évènements 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

Fonctions permettant de répondre à la loi sur l'accessibilité

Loi : « Tout signal lié au fonctionnement d'un dispositif d'accès est sonore et visuel. »
Lors de l'appel, le portier émet un message vocal configurable et la LED de signalisation appel ou un visuel appel sur l'afficheur s'allume.
Lorsque la communication est établie, le portier émet un message vocal configurable et la LED de signalisation communication ou un visuel de communication sur l'afficheur du portier s'allume.
Lors de la commande du relais interne au poste, le portier émet un message vocal configurable et la LED de signalisation « Porte » ou un visuel « Porte » sur l'afficheur du portier s'allume.
Loi : « Lorsqu'il existe un dispositif de déverrouillage électrique, il permet à toute personne à mobilité réduite d'atteindre la porte et d'entamer la manœuvre d'ouverture avant que la porte ne soit à nouveau verrouillée. »
Le relais de gâche du portier est configurable avec un temps de maintien paramétrable.
Loi : « En l'absence d'une vision directe de ces accès par le personnel, les appareils d'interphonie sont munis d'un système permettant au personnel de l'établissement de visualiser le visiteur. »
Les portiers disposent d'une caméra couleur grand angle.
Loi : « Lors de leur installation ou de leur renouvellement, les appareils d'interphonie comportent une boucle d'induction magnétique. »
Les portiers disposent d'une boucle d'induction magnétique intégrée.

FR

EN

CARACTERISTIQUES TECHNIQUES

Conformités aux directives européennes

- 2001/95/EC : Sécurité
- 2014/30/UE : CEM
- 2017/2102/UE : RoHS 3
- 2014/35/UE : Basse Tension
- 2014/53/UE : RED

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 IK09 selon EN 62262
- Degré de protection IP65 selon EN 60529
- Face avant en inox 316L
- Fond encastrable en ABS avec accrochage mural
- Dimensions et poids versions standard :
  - ↘ H 375 x L 145 x P 63 mm
  - ↘ 2Kg
- Dimensions versions grand modèle :
  - ↘ H 493 x L 155 x P 63 mm
  - ↘ 2,5Kg

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

Boutons

- Vitesse d'acquisition 5Hz (200ms)

Entrées

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

Sorties

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

Lecteur

- Fréquence porteuse / Normes SO14443 types A & B, ISO18092 (NFC), Bluetooth
- Compatibilité puces : Bluetooth® Smart (Basse énergie) + MIFARE Ultralight®, MIFARE Ultralight® C, MIFARE® Classic & Classic EV1, MIFARE Plus®, MIFARE® DESFire®, MIFARE® DESFire® EV1 & EV2, NFC HCE, SMART MX, CPS3, iCLASS®, PicoPass®
- Stockage EAL5+
- Interface Wiegand 56bits

FR

EN

Ecran

- Ecran TFT 2,8''
- Résolution : 240 x 320
- Couleur : 262000
- Luminosité : 500cd/m2

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

Vidéo

Caméra :

- Capteur CMOS 1/4'' Full HD 1920 x 1080
- Grand angle 170°
- Vision faible luminosité : 5 Lux minimum à 80 cm

En communication (RTP) :

- Résolutions : QCIF / QVGA / CIF / VGA / HD ou Full HD
- Codecs : H264 / H263-1998 / H263

En vidéo surveillance (RTSP) :

- Résolutions : QVGA / VGA / HD ou Full HD
- Codecs : H264 / MJPEG

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

CASTEL : ZAC de La Ronde – 10 route du Bois de La Casse – 49680 NEUILLE – France
Tél. : (+33) 02.41.40.41.40 - Fax : (+33) 02.41.40.41.49

PRESENTATION

Product references: 590.1060 (XE AUDIO 1B CLAV BLE) - 590.1160 (XE VIDEO 1B CLAV BLE) - 590.6400 (XE AUDIO 1B BLE) - 590.6900 (XE VIDEO 1B BLE) – 590.5500 (XE AUDIO 2B BLE) - 590.6000 (XE VIDEO 2B BLE) – 590.6930 (XE VIDEO 4B BLE) - 590.7400 (XE PAD AUDIO BLE) - 590.7900 (XE PAD VIDEO BLE) – 590.7410 (XE PAD AUDIO CLAV BLE) - 590.7910 (XE PAD VIDEO CLAV BLE) - 591.6000 (XE VIDEO 2B BLE DO) – 591.6900 (XE VIDEO 1B BLE DO) – 591.7900 (XE PAD VIDEO BLE DO)

Your SIP intercom equipment offers the following features (depending on the version):

- Establish audio/video 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
  - ↘ QRCode and barcode reading for automation purposes
- 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 (depending on the version):

- Full HD wide-angle camera, protected by a removable window
- 2.8" TFT screen for viewing and calling names from a directory
- Numerical keypad for dialling and entering an access code
- Integrated access control reader compatible with ISO14443 type A & 3B and Bluetooth allowing :
  - ↘ Either a localized access control at the station
  - ↘ Either supervised access control through the CastelAccess solution
  - ↘ Or supervised access control through the Synchronic solution
  - ↘ Or a third party access control when the terminal output of the reader card is connected for this purpose
- 1 to 2 programmable call buttons for configuring actions of your choice
- 6 "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.
- Compliant with the "law on accessibility for people with disabilities": workstation equipped with pictograms, coloured LEDs, voice synthesizers and a magnetic induction loop.

FR

EN

VERSIONS

- Version 1 PB, 2 PB + multi-technology bluetooth player: Audio only
- Version 1 PB, 2 PB + multi-technology bluetooth reader: Audio and Video
- Version DO 1 PB, 2 PB + multi-technology bluetooth player: Audio and Video, presence of an opening detection contact
- Version Scrolling name + multitechnology bluetooth reader: Audio only
- Version Scrolling name + multi-technology bluetooth reader: Audio and Video
- Version DO Scrolling name + multi-technology bluetooth player: Audio and Video, presence of an opening detection contact
- Version Scrolling name + keyboard + multitechnology bluetooth player: Audio only
- Version Name scrolling + keyboard + bluetooth player multi-technologies: Audio and Video

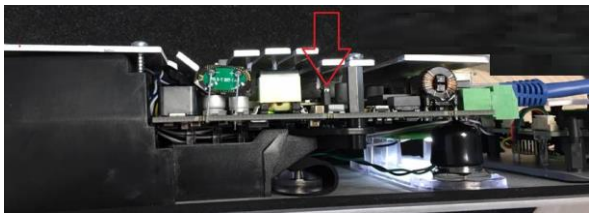
OPTIONS

- Reference 590.9320: Belt for models without numeric keypad
- Reference 590.9500: Cap for models without numeric keypad
- Reference 590.9600: Claw kit for models without numeric keypad (plasterboard mounting)
- Reference 590.9100: Surface-mounted base for models with numeric keypad
- Reference 910.0205 : KIT PROG ARC13.56MHz+BLUETOOTH (necessary for advanced management)
- Reference 910.0206: Virtual Card STid Mobile
- Reference 120.9500: Bluetooth desktop reader

CONNECTION

Power supply connection (24VDC)

The required power supply is 20 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

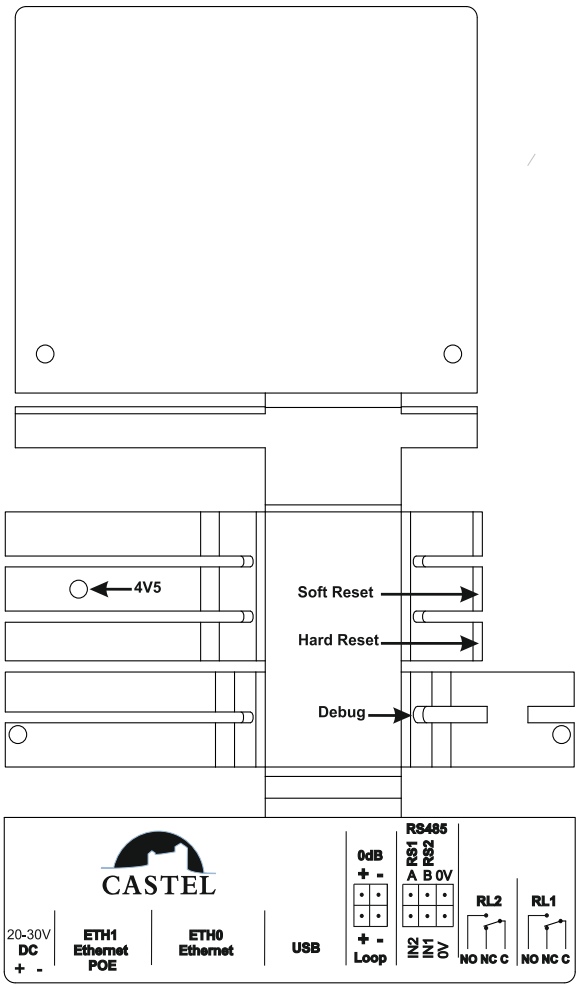


IP network connection (ETH0 / ETH1)

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 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)

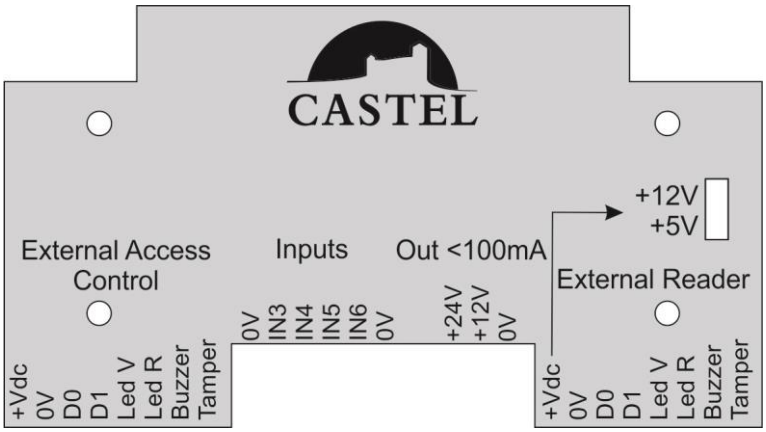
Two digital inputs allow the connection of a dry contact (do not apply voltage). To be activated, the input must be grounded.
The contact can be deported up to 1Km.

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 device to the ground using the terminal provided (Mounted on the fixing of the microphone).



Connection of inputs 3 to 6 (Inputs) *Applicable from software version 1.5.0*

our digital inputs (IN3 / IN4 / IN5 / IN6) allow the connection of a dry contact (do not apply voltage). To be activated, the input must be grounded (0V).
The contact can be deported up to 1Km.

12V or 24V power source for accessories (Out <100mA)

Function only available when the device is powered by PoE+ or an external power supply, it provides a power supply to supply external accessories such as an output BP, a radar, a light in the limit of 24V / 50mA max or 12V / 100mA max

Connecting the external reader (External Reader)

The reader, digital code reader or reader equipped with a connected keyboard can be of type Wiegand (D0 & D1).
Compatible formats are Wiegand 26, 32, 34, 37, 44, 56 and 58 bit
Two open collector outputs allow to control the LED Red (LED R) and Green (LED V) of the reader or digital code connected.
When the device is powered by PoE+ or an external power supply, it can power the external drive (+ Vdc / 0V) within the limit of 5V / 100mA or 12V / 100mA (and up to 200mA if the power supply 12V accessories is not used). For any reader with a higher consumption, provide an external power supply.
The connection is made by wire-to-wire connection, see the data sheet of the connected reader.

Connection of external access control system (External Access Control)

The device's built-in reader has an 8-pin connector for connection to the customer access control system. In this case of use, the reader is no longer managed by the CASTEL device and must be powered by the external access control system.
The maximum distance between the reader and the access control system is 100m max with 6/10 type cable.
Connect one end of the cable screen to ground.
The required power supply (+ VDC / 0V):

- Power supply 9 to 15VDC
- Consumption: 150mA / 12V

The interface is of type Wiegand (D0 & D1) 56 bits.
Two inputs to control the LED Red (LED R) and Green (LED V)
A "Buzzer" input is used to control the reader's buzzer
A "Tamper" output is used to signal the tearing off, do not connect because not available

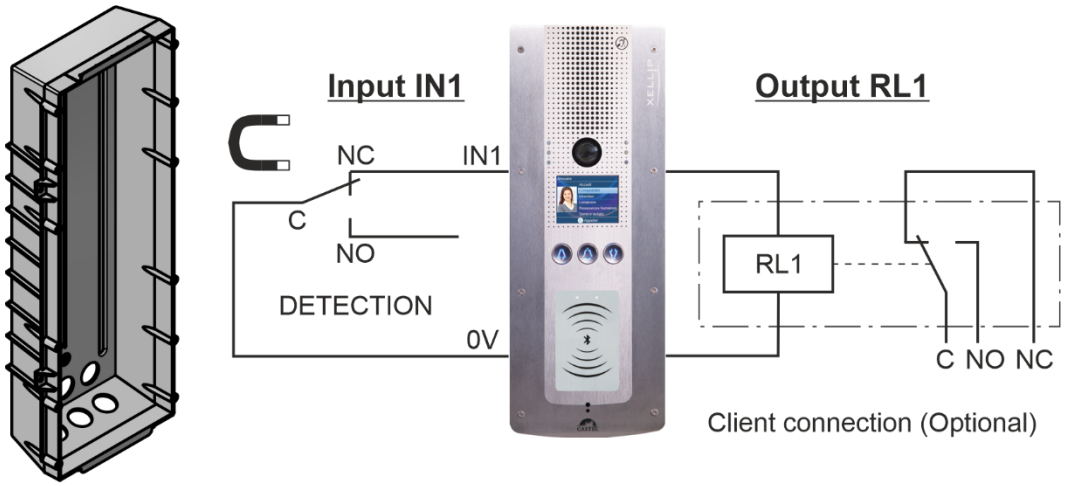
FR

EN

Connection of the opening detection contact (DO version)

DETECTION CONNECTED TO THE BOX

- Opening lift event
- Relay control to be setup

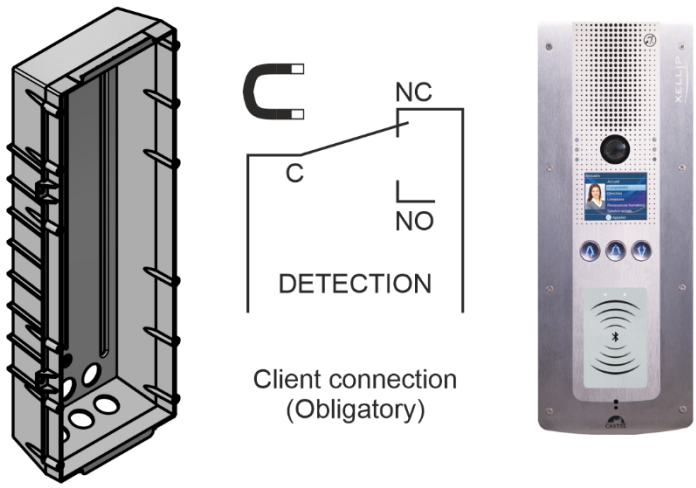


Rear bottom	Detection	Input IN1
Open	NC/C	Activated
Closed	NO/C	Deactivated

NC : Normally Closed
NO : Normally Open
C : Common

DIRECT DETECTION

- No opening feedback on the intercom
- Switching of the magnetic relay on opening
- Direct use of the 20VDC/0.5A contact



Rear bottom	Detection
Open	NC/C
Closed	NO/C

NC : Normally Closed
NO : Normally Open
C : Common

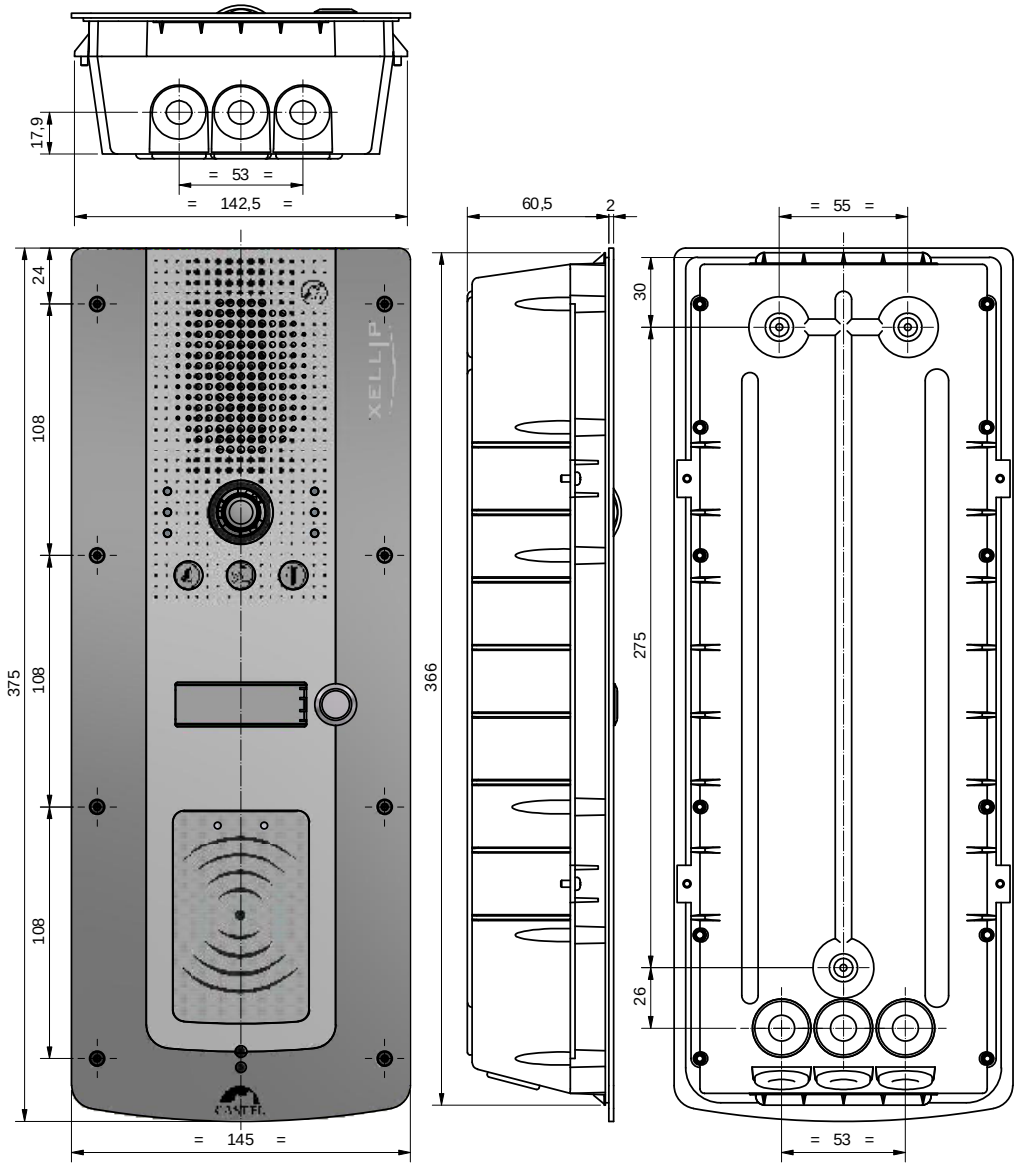
FR

EN

INSTALLATION

Flush mounting of models without numeric keypad

Make a reservation 367mm high, 143mm wide and 65mm deep in the substrate.
Coat the bottom of the recess with at least 10mm of fresh cement.
Insert the base of the doorkeeper into the recess and push it in. Allow the base to protrude 2mm.
Allow the cement to dry for at least 24 hours, then connect the door.
Fix the front panel with the 8 FX (TORX) screws with M3 x 10 studs.
To ensure that your intercom is watertight, it is necessary that the front panel, once mounted, rests on the entire seal between the bottom and the front panel.



Mounting on plasterboard wall

Create a recess 361mm high, 143mm 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 8 FX teat screws (TORX) M3 x 10.

FR

EN

Surface mounting of models without numeric keypad

Fit the bottom on to the Belt (Option ref. 590.9320) using 4 screws CZ M3 x 6.
Attach the assembly (base + belt) on support by three screws of diameter 3 to 3.5 max.
Connect the entry station.
Attach the front panel with the 8 FX teat screws (TORX) M3 x 10.
To ensure that your intercom is watertight, it is necessary that the front panel, once mounted, rests on the entire seal between the bottom and the front panel.

FR

EN

Fitting the cap option to models without numeric keypad

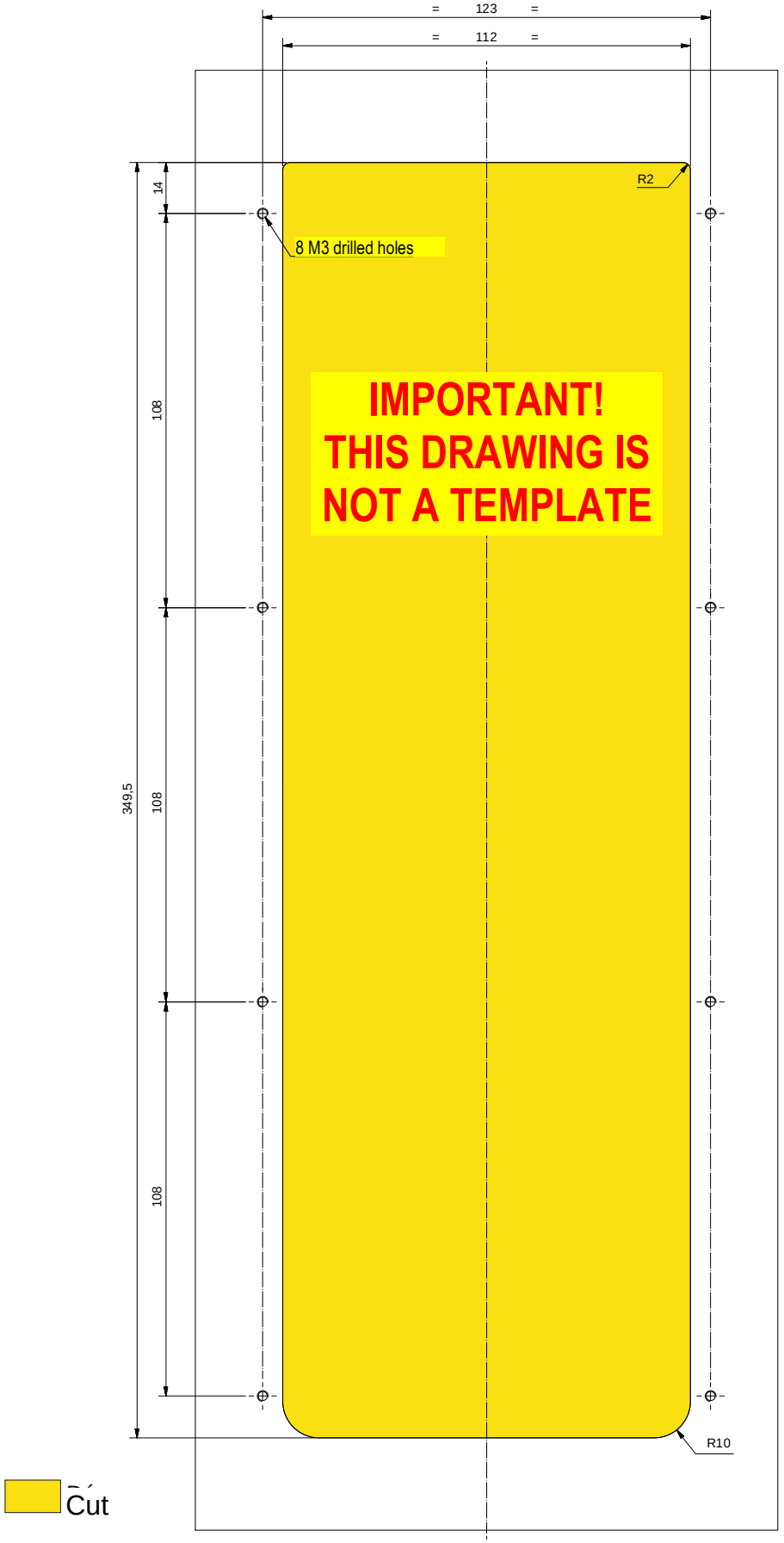
Stainless steel 316L cap. Dimensions: H 370,5mm x W 149mm x D 26mm
Flush bottom.
Attach the cap (Option ref. 590.9500) on the bottom using 4 screws FX (TORX) M3 x 10.
Connect the entry station.
Attach the front panel with the 8 FX teat screws (TORX) M3 x 10.
To ensure that your doorkeeper is watertight, it is necessary that the front panel, once mounted, presses against the entire seal between cap and front panel and between cap and back.

FR

EN

Pole mount for models without numeric keypad

Machine the opening on the post using the drawing below.
Connect the entry station.
Attach the front panel on the post with the 8 FX teat screws (TORX) M3 x 10.
IMPORTANT! The entry station is mounted without a base, the post must be watertight (IP 65).

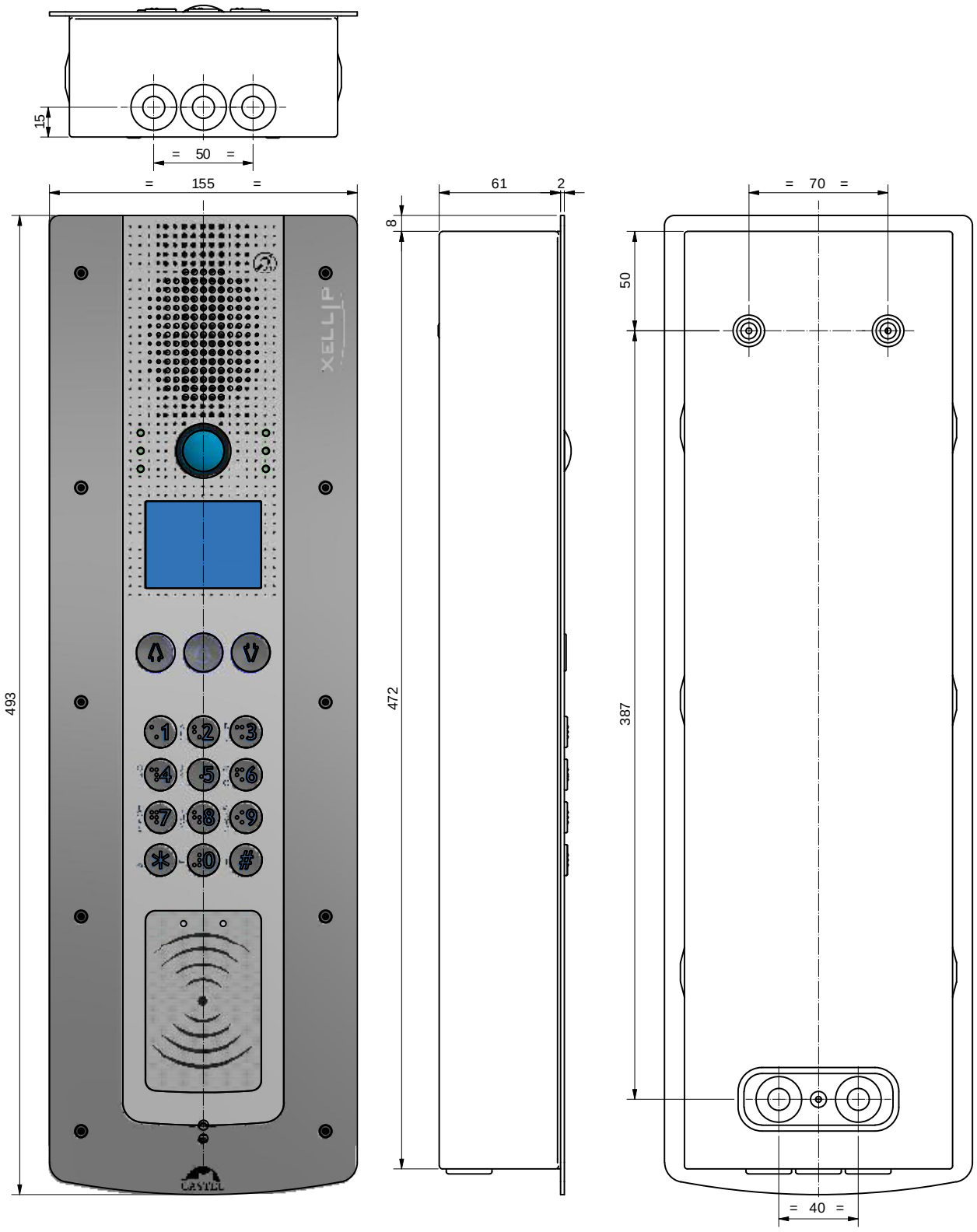


FR

EN

Flush mounting of models with numeric keypad

Make a recess 477mm high, 144mm wide and 65mm deep in the substrate.
Coat the bottom of the recess with at least 10mm of fresh cement.
Insert the bottom of the intercom into the recess and push it in. Allow the base to protrude 2mm.
Allow the cement to dry for at least 24 hours, then connect the door.
Fix the front panel with the 10 FX (TORX) screws with M3 x 10 studs.
To ensure that your intercom is watertight, it is necessary that the front panel, once mounted, rests on the entire seal between the bottom and the front panel.



FR

EN

Surface mounting of models with numeric keypad

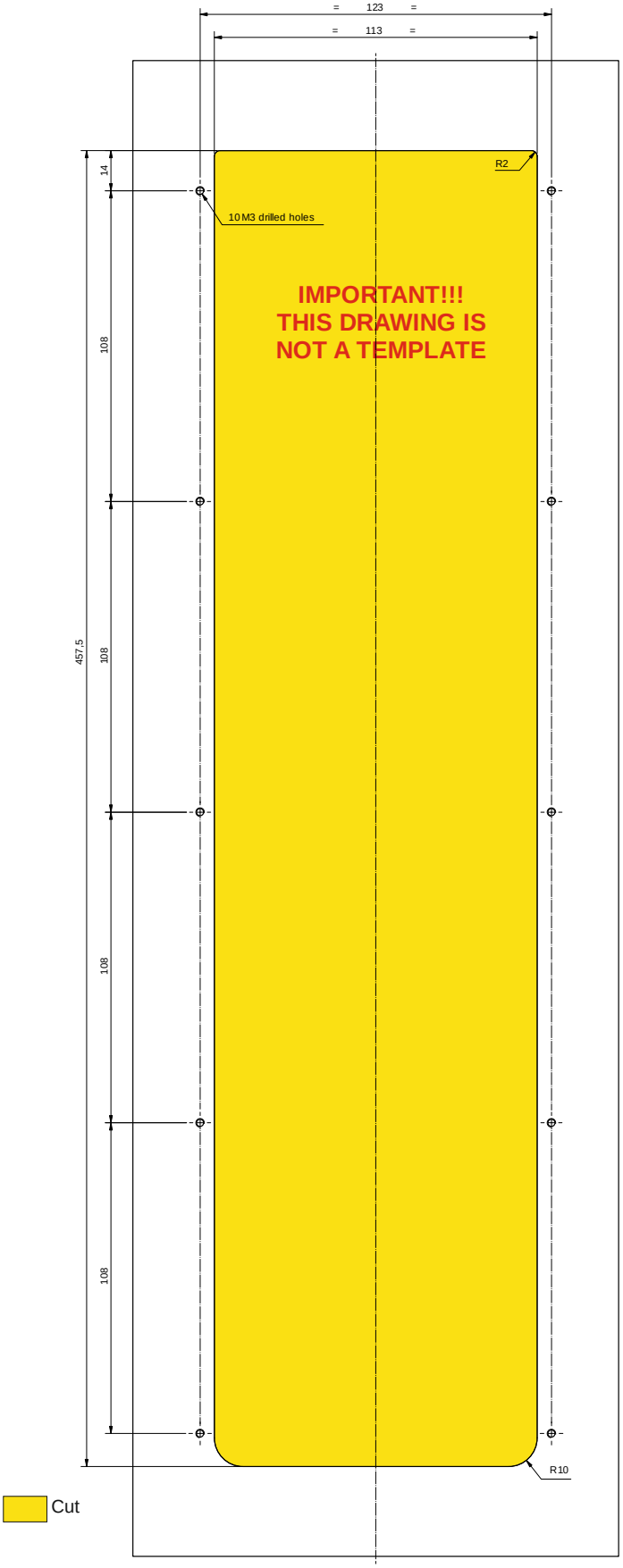
Attach the surface-mounted backplane (Option 590.9100) to its bracket.
Connect the intercom.
Fix the front panel with the 10 FX (TORX) screws with M3 x 10 pins.
To ensure that your intercom is watertight, it is necessary that the front panel, once mounted, rests on the entire seal between the bottom and the front panel

FR

EN

Pole mounting for models with numeric keypad

Machine the opening on the post using the drawing below.
Connect the entry station.
Attach the front panel on the post with the 10 FX teat screws (TORX) M3 x 10.
IMPORTANT! The entry station is mounted without a base, the post must be watertight (IP 65).



FR

EN

USE

Station IP address

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 :

- CastelIPSearch 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

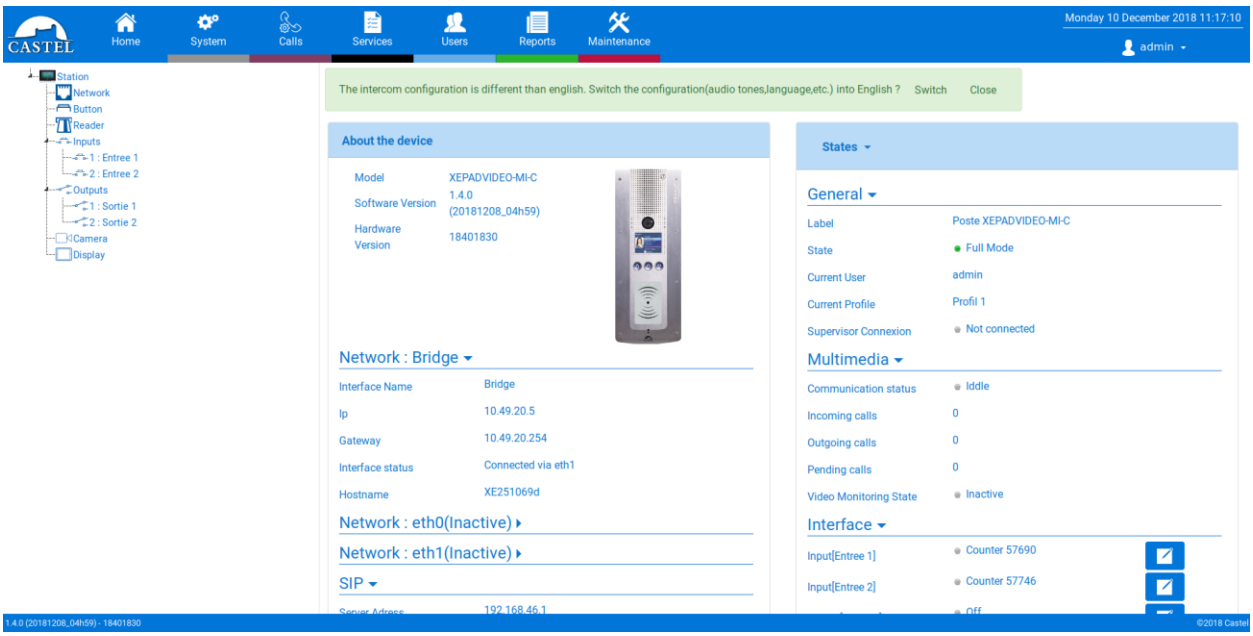
When the "Soft Reset" button is pressed and held for more than 20 seconds, the terminal is restarted and the parameters are reset to the factory configuration.
Pressing the "Hard Reset" button only restarts the terminal immediately.

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]
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.

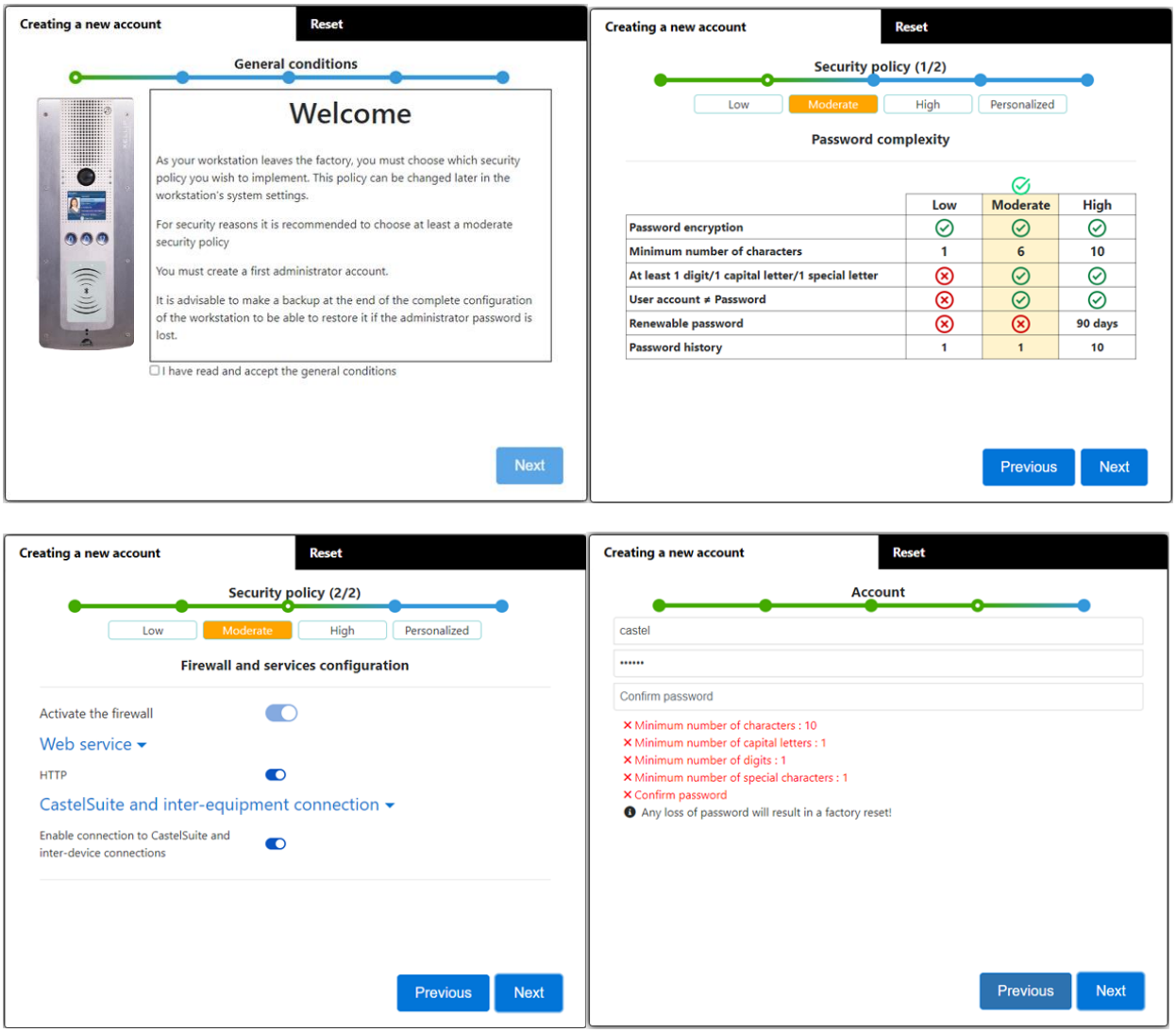


FR

EN

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

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



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

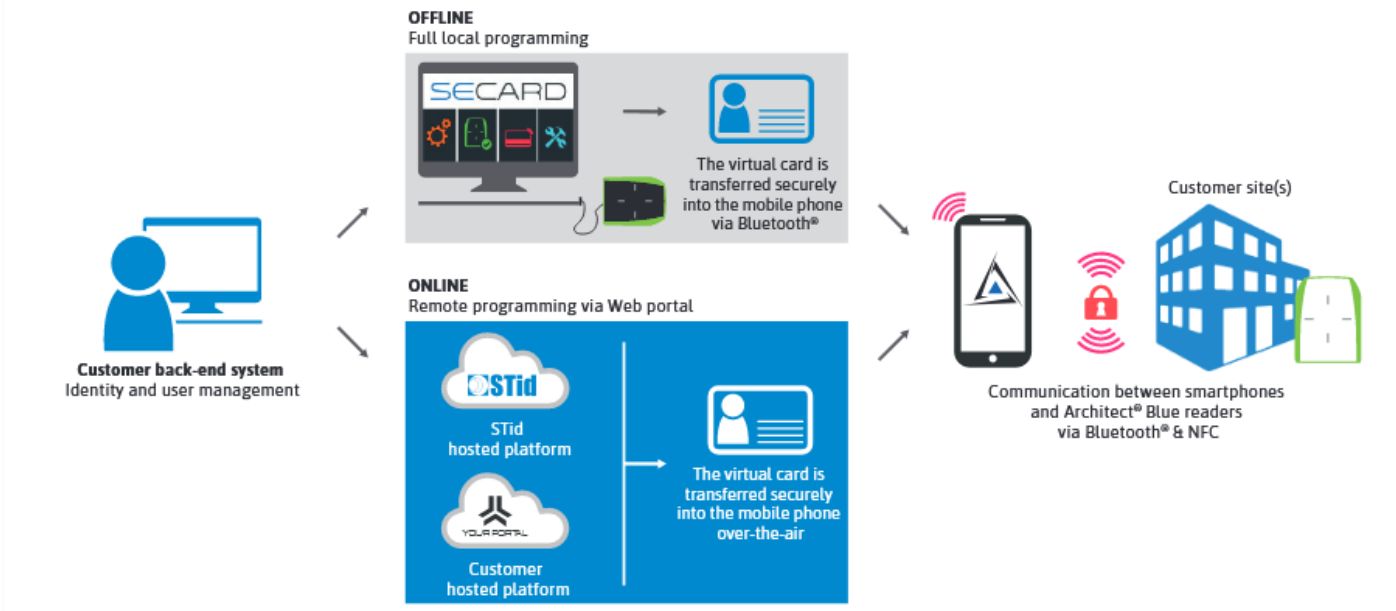
Your CASTEL product must only be cleaned using a mild cleaning product (water or soapy water) that is non-abrasive, non-foaming and above all free from any type of solvent or alcohol.
For regular maintenance, only use water, without detergent.
Jet cleaning must be prohibited, as well as use of abrasive sponges and cloths with aggressive surfaces.

FR

EN

USING THE BLUETOOTH SOLUTION

Integration of the solution



The secure and user-friendly identification solution STid Mobile ID® transfers the access badge to Android ™ and iOS® smartphones, in addition to or replacement of the traditional RFID card.
It includes a free mobile application, the latest generation of multi-technology readers and Offline and Online configuration tools.

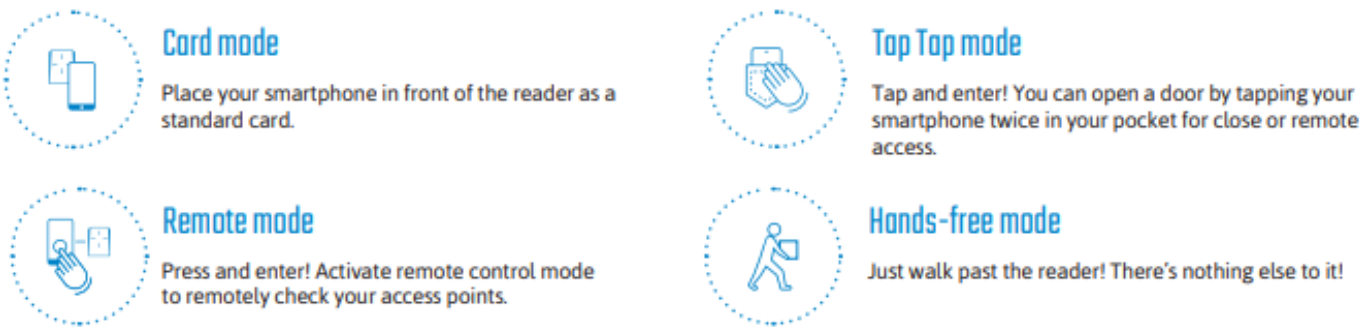
Offline mode

- Full local programming via SECard tool
- Full control over security and configuration settings
- Plug & Play without any development required

Online mode

- GDPR certified data storage on server based in France
- Secure Web portal and secure exchanges - HTTPS & TLS
- Database encryption and fragmentation
- Dynamic rights management: remote creation, revocation and update
- Simplified visitor management with unlimited reuse of revoked badges
- Alignment with our clients' value chain via sub-account management
- Different levels of rights for each account
- Customizable user cards

Bluetooth access control mode



Mobile Apps

STid Moblie ID

- The STid Mobile ID® app is a virtual wallet of access badges. It can receive and store an unlimited number of virtual cards. Each virtual card carries a secure identifier, programmed by the client / user or predefined.
- STid Mobile ID® is downloadable on the Google Play (Android) and App Store (iOS) platforms. 95% of the smartphones on the market work with one of these two operating systems
- The STid Mobile ID® app is free. A free CSN virtual card - STid Mobile ID® - is directly stored in the application with a unique number assigned to the installation.

STid Settings

- STid Settings is a virtual wallet of configuration cards for storing them in your smartphone and setting up readers with ease
- STid Settings is available for download on Google Play (Android) and App Store (iOS) platforms. 95% of smartphones on the market work with one of these 2 operating systems
- The STid Settings app is free.

Virtual cards

A virtual card is the dematerialization of your card access control within a mobile application. Your virtual card has an identifier and behaves like an RFID badge
There are 3 types of access card adapted to your needs:

CSN STid Mobile ID:

- Unique number provided to the installation
- Authorized mode: card mode
- Cost: Free, provided with STid Mobile ID app

CSN STid Mobile ID+:

- Unique number provided to the installation
- Authorized mode: card mode, Tap Tap, hands-free.
- Cost : 1 credit

Virtual Access Card

- Private ID
- Fully configurable security parameters
- Authorized mode: card, Tap Tap , hands-free, remote.
- Cost : 5 credits

Reader configuration

The reader is pre-configured to read the serial number of the Mifare Classic, Mifare Plus, Mifare UltraLight, Mifare DESFire, Blue, CPS3 and ISO14443B-3B badges.
Three configuration card (SCB) provided with the device enable the bluetooth access control modes:

- Card + Mode Contact
- Card + Mode Contact + Tap-Tap
- Card + Mode Contact + Handsfree.

The set of configurable parameters of the reader are accessible with the programming kit KIT PROG ARC13.56MHz + BLUETOOTH (ref 910.0205)
If the SCB is compatible with the player's firmware, the buzzer will sound 5 times.
If the SCB is not compatible with the player's firmware, the buzzer is activated 1s.

FUNCTIONS

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

Video interface functions

- Configure video communication parameters: RTP port, video codecs (H264 / H263 & H263+)
- Configure resolution (QCIF / QVGA / CIF / VGA / HD / Full HD)
- Ability to manage communication bandwidth
- Ability to adjust camera settings

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

'Scroll call' button functions

- This button is the main button of stations with name scrolling module.
- Generally, it can confirm the current action.
- When the entry station is idle, this button can be programmed to call 1 to 10 stations simultaneously or with timeout and display a help menu on how to use the entry station.

Badge reader functions

- Configure the type of badge.
- Inhibit the reader
- Perform access control :
  - ↘ Either localized at the station
  - ↘ Either supervised through the CastelAccess solution
  - ↘ Or supervised through the Synchronic solution

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.

Directory configuration

Station directory inputs can be created, modified or deleted.
It is possible to create inputs for simple calls or multiple calls

Local access configuration

It is possible to configure a simplified access control on the station:

- Programming from 1 to 45,000 access codes of 1 to 20 figures.
- Programming action or actions associated with access authorisation and denial by logical relations.
- Recognition of 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

QRCode and barcode function

The set supports QRCode and barcode reading when the video RTSP service is not enabled.
This feature can be enabled or disabled depending on the profile.
The following barcode formats are supported: EAN-8, EAN-13 (and its derivatives ISBN-10, ISBN-13...), I2/5, Code-39 and Code-128.
Automations can be triggered by the detection of a QRCode or barcode in the relationships.

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

Functions used to meet the accessibility law (depending on versions)

Rule: 'Any signal related to the operation of an access device is audible and visual.'
During the call, the entry station sends a configurable voice message and the call signal LED or a call visual on the display switches on.
When the call is going through, the entry station sends a configurable voice message and the call signal LED or a call visual on the entry station display switches on.
During the internal relay command at the station, the entry station sends a configurable voice message and the door signal LED or a door visual on the display switches on.
Rule: 'When there is an electric unlocking device, it enables any person with reduced mobility to reach the door and start the opening manoeuvre before the door becomes locked again.'
The entry station's strike plate relay can be configured with a configurable hold time.
Rule: 'In the absence of a direct view of these accesses by staff, the intercom devices feature a system enabling staff to view the visitor.'
The entry stations have a wide-angle colour camera.
Rule: 'When they are installed or renewed, the intercom devices have a magnetic induction loop.'
Entry stations have an integrated magnetic loop.

TECHNICAL CHARACTERISTICS

Compliance with european directives

- 2001/95/EC: Safety
- 2014/30/UE: EMC
- 2017/2102/EU: RoHS 3
- 2014/35/EU: Low voltage
- 2014/53/UE: RED

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

- IK09 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 and Weight standard versions :
  - ↘ H 375 x W 145 x D 63 mm
  - ↘ 2kg
- Dimensions and Weight large versions:
  - ↘ H 493 x W 155 x D 63 mm
  - ↘ 2,5Kg

General electric characteristics

- Operating temperature: -20° to +50°C.
- Storage temperature -20° to +70°C.
- Relative humidity: <90%, without condensation.
- External power :
  - ↘ 24VDC (20 à 30VDC) 30W max
- Power PoE IEEE 802.3af 12,9W max
- Power PoE+IEEE 802.3at 25,5W max

Buttons

- Acquisition speed 5Hz (200ms)

Inputs

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

Outputs

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

Lecteur

- ISO14443 types A & B, ISO18092 (NFC), Bluetooth
- Compatibility : Bluetooth® Smart (Basse énergie) + MIFARE Ultralight®, MIFARE Ultralight® C, MIFARE® Classic & Classic EV1, MIFARE Plus®, MIFARE® DESFire®, MIFARE® DESFire® EV1 & EV2, NFC HCE, SMART MX, CPS3, iCLASS®, PicoPass®
- Storage EAL5+
- Wiegand 56bits

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

Video

Camera:

- 1/4" Full HD 1920 x 1080 CMOS sensor
- 170° wide angle
- Low light vision: 5 Lux minimum at 80cm

In communication (RTP):

- Resolutions: QCIF / QVGA / CIF / VGA / HD or Full HD
- Codecs: H264 / H263-1998 / H263

In video surveillance (RTSP):

- Resolutions: QVGA / VGA / HD or Full HD
- Codecs: H264 / MJPEG

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

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

CASTEL: ZAC de La Ronde – 10 route du Bois de La Casse – 49680 NEUILLE – France
Tel.: +33 (0)2.41.40.41.40 - Fax: +33 (0)2.41.40.41.49