



CYBERSÉCURITÉ

GUIDE DE RENFORCEMENT

Comment prévenir ou réduire l'impact des risques de sécurité.

v.2.0

La communication est cruciale dans tous les domaines d'activité. Les renseignements exploitables sont essentiels à la prise de décision qui favorise l'efficacité opérationnelle.

Lorsque la communication nécessite un système audio vocal, sa clarté doit passer au premier plan. On ne peut pas se permettre de se tromper de message, ce qui entraînerait un risque fort pour votre modèle commercial.

Depuis plus de 70 ans, le groupe Zenitel propose des innovations qui résolvent ce problème, en veillant à ce que chacun puisse entendre, être entendu et compris, à tout moment et partout.



TABLE DES MATIÈRES

CYBERSÉCURITÉ.....	4
Faire face aux problèmes de cybersécurité	4
Se protéger contre les cyberattaques.....	4
Adhésion au CIS (Center for Internet Security).....	4
Mettre en place des bases solides.....	5
Planification de la cybersécurité.....	5
Les principaux éléments constitutifs	5
PLANIFIER.....	8
Degrés de risque et de sécurité	8
Mécanismes de sécurité	9
CONTRÔLE CIS 4 : utilisation contrôlée des privilèges administratifs.....	10
Gestion des mots de passe et identifiants.....	10
Outils de gestion des mots de passe et identifiants	10
CONTRÔLE CIS 9 : limitation et contrôle des ports, protocoles et services du réseau	11
DÉPLOYER	12
Installer et mettre en place la cybersécurité	12
Installation et configuration de dispositifs d'interphonie IP pour la cybersécurité.....	12
Installation et configuration du serveur ICX 500 et AlphaCom XE pour la cybersécurité.....	16
CONTRÔLER.....	20
Remplir la liste de vérification du système de cybersécurité	20
AGIR.....	21
Évaluer et assurer le suivi.....	21
POUR EN SAVOIR PLUS.....	22
Téléchargements, informations générales, CIS, service client	22

CYBERSÉCURITÉ

“La grande majorité des problèmes de cybersécurité peuvent être évités par des actions proactives, des technologies et des pratiques déjà à disposition.”

L'accès au réseau offre de nombreux avantages à votre personnel et à votre entreprise. Toutefois, plus vous accordez d'accès, plus grand est le risque de voir les vulnérabilités accrues exploitées par des individus extérieurs. La cybersécurité est la clé pour garantir un cyberenvironnement sûr, stable et résistant.

Faire face aux problèmes de cybersécurité

Chaque ajout de nouveau système, application ou service réseau s'accompagne de vulnérabilités potentielles en matière de sécurité, ce qui rend la cyberprotection de plus en plus difficile et complexe. En abordant de manière pragmatique les risques sérieux liés à la sécurité du réseau, vous pouvez en tirer des avantages tout en minimisant ces risques. Pour y parvenir, il vous faut un plan de cybersécurité solide et les ressources nécessaires pour l'exécuter. La réduction des risques de cybersécurité en amont nécessite généralement moins de ressources que le nettoyage après des cyberattaques évitables..

Se protéger contre les cyberattaques La grande majorité des problèmes de cybersécurité peuvent être évités par des actions proactives, des technologies et des pratiques déjà à disposition. Pourtant, de nombreuses organisations sont submergées par le "fog of more" : plus de travail, de problèmes, d'exigences réglementaires et de conformité, d'opinions contradictoires, de bruit sur le marché et de recommandations peu claires ou décourageantes que quiconque peut gérer. Même au sein des rares entreprises disposant des informations, de l'expertise, des ressources et du temps nécessaires pour faire le tri, il est rare que ce soit le cas pour tous leurs partenaires commerciaux, fournisseurs et clients clés.

Adhésion au CIS Le "Center for InternetSecurity"

(Centre pour la sécurité d'Internet) est une entité à but non lucratif tournée vers l'avenir qui exploite la puissance de la communauté informatique mondiale pour protéger les organisations privées et publiques contre les cybermenaces. Ses contrôles CIS Version 7.1 et CIS Benchmarks constituent la norme mondiale et les meilleures pratiques reconnues pour sécuriser les systèmes et les données informatiques contre les attaques les plus répandues. Les contrôles CIS s'alignent sur tous les principaux cadres de conformité, tels que le NIST Cybersecurity Framework, les directives du NIST et la série ISO 27000, ainsi que sur les réglementations, notamment PCI, DSS, HIPAA, NERC CIP et FISMA.

Une communauté mondiale bénévole de professionnels de l'informatique expérimentés affine et vérifie en permanence ces directives éprouvées. Le CIS abrite le

Multi-State Information Sharing & Analysis Center (MS-ISAC®), la ressource de référence pour la prévention, la protection, la réponse et la récupération des cybermenaces pour les gouvernements des États, des collectivités locales, des tribus et des territoires.

Zenitel est fière d'être membre de CIS SecureSuite, ce qui nous permet de renforcer nos défenses en matière de cybersécurité en tirant parti de l'expertise et des ressources de CIS pour nous protéger contre les cyberattaques les plus répandues et les plus dangereuses.

Mettre en place des bases solides

Les contrôles CIS sont divisés en ce que CIS appelle « Fondation de base » et « Organisationnel ».

Outre les contrôles de base (1 à 6), un système de cyberdéfense efficace doit respecter les cinq principes fondamentaux suivants :

L'attaque éclaire la défense : Utiliser les connaissances tirées des attaques réelles ayant compromis les systèmes pour fournir la base nécessaire afin d'apprendre continuellement de ces événements et construire des défenses efficaces et pratiques. N'incluez que les contrôles dont on peut prouver qu'ils stoppent les attaques réelles connues.

Priorisation : Investir d'abord dans les contrôles qui vous permettront de réduire au maximum les risques et de vous protéger contre les acteurs les plus dangereux pouvant être mis en œuvre dans votre environnement informatique. Les groupes de mise en œuvre du CIS présentés ci-dessous constituent un excellent point de départ pour les organisations qui souhaitent identifier les sous-contrôles pertinents.

Mesures et paramètres : Établir des paramètres communs afin de fournir un langage partagé aux dirigeants, aux spécialistes des TI, aux auditeurs et aux responsables de la sécurité pour mesurer l'efficacité des mesures de sécurité au sein d'une organisation, de sorte que les ajustements nécessaires puissent être identifiés et mis en œuvre rapidement.

Diagnostic et réduction des risques en continu : Effectuer des évaluations continues pour tester et valider l'efficacité des mesures de sécurité actuelles et pour aider à déterminer la priorité des prochaines étapes.

Automatisation : Automatiser les défenses afin de permettre aux organismes d'obtenir des mesures fiables, évolutives et continues de leur application des contrôles et mesures connexes.

D'après les directives du CIS, il est également essentiel de prendre une décision formelle, consciente et de haut niveau pour intégrer les contrôles du CIS dans la norme de cybersécurité de toute organisation.

La direction et le conseil d'administration doivent également apporter leur soutien et leur responsabilité, en demandant la mise en œuvre des contrôles fondamentaux du CIS dans leur organisation, comme exigence minimale.

Vous trouverez de plus amples informations sur le cadre des contrôles critiques de sécurité du CIS sur le site <https://www.cisecurity.org/controls/>

REMARQUE :

Ce guide couvre la passerelle ICX-500 et les séries de serveurs ICX-AlphaCom et AlphaCom XE, ainsi que tous les appareils d'interphone IP Zenitel, à l'exception du téléphone vidéo ITSV-1. Sauf mention explicite, les outils de bureau tels que AlphaPro, AlphaView, VS-Recorder et VS-Intercom Management Tool ne sont pas inclus.

CIS SecureSuite
Membership



LES PRINCIPAUX ÉLÉMENTS CONSTITUTIFS:



PLANIFICATION DE LA CYBERSÉCURITÉ

Il est important de considérer et comprendre ce qui est essentiel pour votre entreprise et pour les systèmes et solutions que vous utilisez. A partir de là, vous pouvez planifier, mettre en œuvre et gérer votre défense en matière de cybersécurité.

Zenitel a développé ce Guide de renforcement de la cybersécurité pour vous aider à aborder votre planification, sur la base des contrôles CIS. Il combine notre expérience de l'application des meilleures pratiques développées par le CIS pour aider les utilisateurs finaux et les intégrateurs à construire une bonne cyberdéfense.

Nous recommandons aux organisations de suivre les groupes de mise en œuvre du CIS pour les aider à hiérarchiser leur stratégie en fonction de leur adéquation avec les 3 groupes de mise en œuvre suivants :

GRUPE DE MISE EN ŒUVRE 1 (IG1) :

Une organisation IG1 est généralement de taille petite à moyenne, avec une expertise limitée en matière d'informatique et de cybersécurité à consacrer à la protection des actifs informatiques et du personnel. La principale préoccupation de ces organisations est de maintenir l'activité opérationnelle, car elles ont une tolérance limitée aux temps d'arrêt. Une entreprise familiale comptant de 10 à 50 employés peut se classer dans la catégorie IG1.

GRUPE DE MISE EN ŒUVRE 2 (IG2) :

Les organisations IG2 sont en général de taille moyenne à grande et emploient des personnes responsables de la gestion et de la protection de l'infrastructure informatique. Ces organisations soutiennent de multiples départements ayant des profils de risque différents. Les organisations IG2 stockent et traitent souvent des informations sensibles sur les clients ou les entreprises et peuvent supporter de courtes interruptions de service. Certaines organisations de petite ou moyenne taille qui seraient normalement considérées comme IG1 mais qui sont responsables de la protection des données sensibles pourraient donc faire partie de ce groupe supérieur.

GRUPE DE MISE EN ŒUVRE 3 (IG3) :

Une organisation IG 3 sera généralement un organisme public ou une grande entreprise comptant des milliers d'employés. Les IG3 emploient des experts en sécurité qui se spécialisent dans les différentes facettes de la cybersécurité, telles que la gestion des risques, les tests de pénétration et la sécurité des applications. Les systèmes et les données des IG3 ont tendance à contenir des informations sensibles ou des fonctions qui font l'objet d'une conformité et d'une surveillance réglementaires. Les attaques réussies peuvent causer des dommages importants au bien-être public. L'IG3 doit donc se concentrer sur la disponibilité, la confidentialité et l'intégrité des données et sur les attaques d'un adversaire sophistiqué.



PLANIFIER

NIVEAUX DE RISQUE ET DE SÉCURITÉ

Les niveaux de risque et de sécurité varient d'un organisme à l'autre. Les facteurs suivants peuvent avoir un impact sur ces niveaux :

1.

Le nombre d'administrateurs qui auront accès aux systèmes.

Un système comportant de nombreux administrateurs présente un risque plus élevé que les mots de passe tombent entre de mauvaises mains ou que d'autres choses puissent mal tourner en matière de cybersécurité.

2.

Ressources disponibles et niveaux d'expertise.

Une entreprise disposant de plus de ressources informatiques dédiées et sensibilisées à la cybersécurité sera en mesure de mettre en œuvre davantage de contrôles et les rendre plus efficaces dans l'ensemble de l'organisation.

3.

Le niveau de menace général auquel est soumis votre organisation.

Les entreprises qui protègent des actifs de grande valeur ou des données sensibles, ou qui fournissent des infrastructures critiques ou des services publics, courent un risque plus élevé de voir des intrus mieux équipés tenter de percer leurs cyberdéfenses.

MÉCANISMES DE SÉCURITÉ

Le tableau suivant présente les mécanismes de sécurité pertinents pour chaque niveau de système, classés par contrôle CIS.

CONTRÔLE CIS	Groupe de mise en œuvre :		
	IG1	IG2	IG3
Contrôle 1 : inventaire des dispositifs autorisés et non autorisés			
Réseau propre dédié aux dispositifs de sécurité physique.			
Maintenir un inventaire des dispositifs accédant au réseau.			
Utilisez des outils d'inventaire tels que la journalisation DHCP, 802.1x avec comptabilité radius, les outils de découverte automatique, etc. pour maintenir un inventaire à jour.			
Déployer l'authentification au niveau du port via 802.1X pour limiter et contrôler les dispositifs pouvant accéder au réseau.			
Utiliser des certificats pour 802.1X.			
Résoudre les problèmes de ressources non autorisées.			
Contrôle 2 : inventaire des logiciels autorisés et non autorisés			
Vérifier que vous disposez du dernier logiciel de production pour les produits Zenitel auprès de votre intégrateur.			
Maintenir un inventaire détaillé des logiciels autorisés nécessaires sur le réseau.			
Utiliser un outil d'inventaire des logiciels pour suivre les logiciels en cours d'exécution sur tous les appareils.			
Résoudre les problèmes de logiciels non autorisés.			
Contrôle 3 : gestion continue des vulnérabilités			
Exécuter les outils d'analyse automatisée des vulnérabilités.			
Déployer les outils de gestion automatisée des correctifs logiciels.			
Contrôle 4 : utilisation contrôlée des privilèges administratifs			
Changer les mots de passe par défaut sur les terminaux et serveurs.			
Assurer l'utilisation de comptes administratifs dédiés pour la gestion de l'interphone.			
Utiliser des mots de passe uniques (pour plus d'informations, voir page suivante - Contrôle du CIS 4.)			
Tenir un inventaire détaillé des comptes administratifs.			
Contrôle 6 : maintenance, surveillance et analyse des journaux d'audit			
Activer l'enregistrement de l'audit.			
Activer le protocole NTP dans les appareils finaux (interphone IP) pour vous assurer que tous les événements sont enregistrés avec l'heure correcte.			
Activer SNMP syslog pour envoyer les événements aux serveurs d'enregistrement.			
Examiner régulièrement les journaux pour identifier les anomalies.			
Contrôle 9 : limitation et contrôle des ports, protocoles et services du réseau			
Veiller à ce que seuls les ports, protocoles et services, répondant à des besoins commerciaux validés, soient appliqués.			
Appliquer des pare-feux basés sur l'hôte ou des outils de filtrage de port avec une règle de refus par défaut pour supprimer le trafic de tous les ports et services autres que ceux qui sont spécifiquement autorisés.			
Passez en revue les protocoles qu'il faut envisager d'ouvrir à partir du réseau physique dédié vers d'autres réseaux d'entreprise. (Voir page 11: Contrôle CIS 9).			
Contrôle 10 : capacités de récupération des données			
Fournir une sauvegarde de la configuration des appareils d'interphone IP.			
Contrôle 11 : configuration sécurisée des dispositifs de réseau (pare-feu, routeurs et commutateurs)			
Installer la dernière version stable de toutes les mises à jour liées à la sécurité sur tous les appareils.			



CONTRÔLE CIS 4 : utilisation contrôlée des privilèges administratifs

Gestion des mots de passe et identifiants

Pour gérer les mots de passe, vous devez avoir une politique en matière de mots de passe qui précise la force du mot de passe et la fréquence à laquelle il doit être renouvelé. Un mot de passe fort est long - plus il est long, mieux c'est - et se compose d'une combinaison de caractères spéciaux peu susceptibles d'être devinés par des personnes extérieures.

Pour nos appareils d'interphonie IP, la passerelle ICX 500 et les serveurs ICX-AlphaCom / AlphaCom XE, Zenitel recommande l'utilisation de :

- Des mots de passe forts (jusqu'à 20 caractères).
- Des mots de passe générés de façon aléatoire.

Les identifiants de connexion des appareils d'interphonie et des serveurs AlphaCom sont rarement utilisés après la configuration initiale. Le besoin de changer et de renouveler les mots de passe n'est donc pas aussi élevé que celui des mots de passe utilisés quotidiennement. Envisagez d'utiliser le même mot de passe de connexion pour le portail de configuration Web sur tous les appareils afin de réduire les difficultés de mise en œuvre et de gestion des mots de passe. Toutefois, pour maintenir la sécurité, seuls quelques administrateurs devraient alors disposer de ces informations d'identification et les utiliser.

Outils de gestion des identifiants et mots de passe

Pour créer des identifiants pour les appareils d'interphonie et les serveurs, vous devez utiliser un générateur de mots de passe. Le mot de passe doit comporter un minimum de 12 caractères, mais nous recommandons 20 caractères. Vous trouverez un bon exemple de générateur de mots de passe sur <https://strongpasswordgenerator.com>. Les générateurs de mots de passe rendent les informations d'identification plus difficiles à pirater.

Il est facile d'oublier des mots de passe forts, et nous avons vu des exemples d'utilisateurs qui avaient affiché leurs mots de passe sur des Post-It sur leur bureau. Ce n'est évidemment pas idéal du point de vue de la sécurité.

Pour stocker les mots de passe, nous recommandons l'utilisation d'un programme de gestion des mots de passe comme KeePass, qui est un logiciel libre, gratuit à utiliser (<http://keepass.info>). L'application stocke les identifiants de connexion dans une base de données chiffrée. Bien entendu, le mot de passe de la base de données elle-même doit être très fort et ne pas être facile à retenir. Mais il se peut que vous ayez besoin de vous connecter quotidiennement à cette base de données avec un mot de passe dont vous pouvez vous souvenir.

CONTRÔLE CIS 9 : limitation et contrôle des ports, protocoles et services du réseau

Les solutions de communication IP de Zenitel utilisent les ports, protocoles et services IP suivants :

Tableau 1 - Ports TCP et services

SERVICE	PORT #	DESCRIPTION
AlphaNet Data	50000	Communication de données entre les serveurs ICX-AlphaCom et les systèmes externes
AlphaPro	60001	Utilisé entre AlphaPro et l'outil PC AlphaPro
AlphaVision	55010	Utilisé entre AlphaPro et l'outil PC VS Operator
Démo	50010	Utilisé uniquement pour les applications de démonstration
Serveur DNS	53	Service de recherche DNS sur TCP
HTTP	80	Utilisé pour les communications Web et IMT
HTTPS	443	Utilisé pour le web
Postes IP	50001	Utilisé entre le serveur ICX-AlphaCom et les interphones IP
Multimodule Data	50010	Utilisé entre les modules maître et esclave du serveur ICX-AlphaCom
Serveur OPC 1	61112	Utilisé entre le serveur ICX-AlphaCom et les serveurs OPC
Serveur OPC 2	61113	Utilisé entre les serveurs ICX-AlphaCom et OPC
SIP	5060	Uniquement pour les interphones SIP se connectant à des serveurs SIP
SIPS	5061	Uniquement pour les interphones SIP se connectant à des serveurs SIP
SSH	22	Utilisé pour la communication SSH
ZAP	50004	Utilisé pour l'intégration entre les appareils VS en mode SIP/ Edge et les systèmes externes
ZAP Web	8080	Utilisé pour lire les informations ZAP

Tableau 2 - Ports UDP et services

SERVICE	PORT #	DESCRIPTION
Données audio	5035	Utilisé uniquement pour la démo
Client DHCPv4	68	Communications avec le serveur DHCP
Serveur DHCPv4	67	Alternative à l'utilisation de ICX-AlphaCom comme serveur DHCP
DIP multicast	5001	Signalisation d'appel de groupe pour ICX-AlphaCom vers des dispositifs IP
Discovery	5002	Protocole de découverte pour les dispositifs d'interphonie IP
Serveur DNS	53	Recherche de DNS sur UDP
mDNS	5353	
Serveur NTP	123	Synchronisation de l'heure avec les serveurs NTP
SIP	5060	Signalisation SIP vers les serveurs SIP et les appareils en mode EDGE
Pulse	5062	Port SIP supplémentaire utilisé en mode EDGE
SNMP	161	Interface avec les serveurs SNMP
TFTP	69	Utilisé pour la mise à jour du firmware et le provisionnement automatique
VoIP audio	61000:61250	Transfert des charges utiles audio et vidéo



DÉPLOYER

INSTALLER ET METTRE EN PLACE LA CYBERSÉCURITÉ

Une fois que vous avez terminé la phase de planification pour assurer la cybersécurité de votre système, il est temps de passer à la mise en œuvre. Une partie importante de celle-ci consiste à configurer correctement votre appareil ou système. Nous vous proposons ici deux séries d'instructions : l'une sur l'installation et la configuration des dispositifs d'interphonie IP et l'autre sur l'installation et la configuration d'un serveur ICX-AlphaCom / AlphaCom XE.

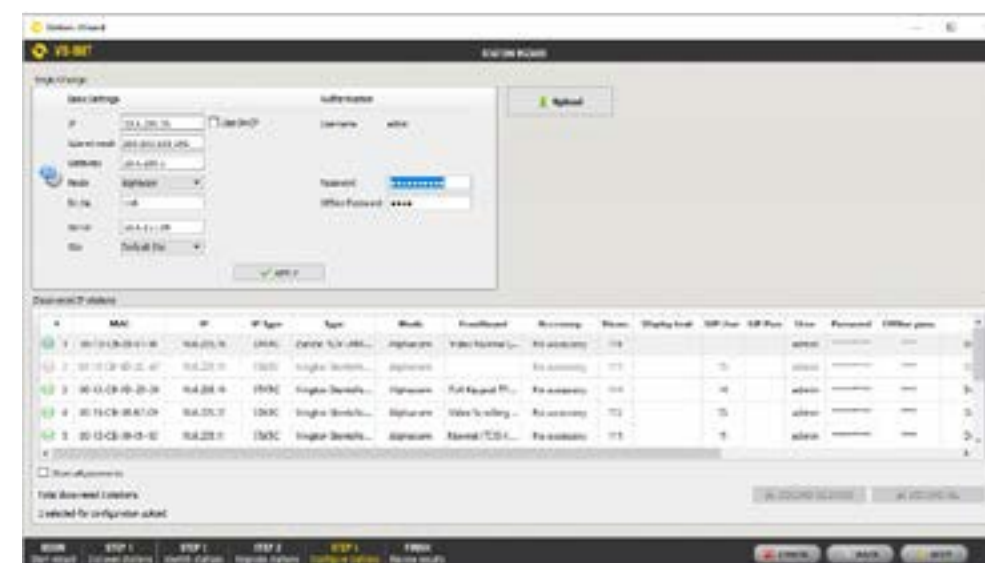
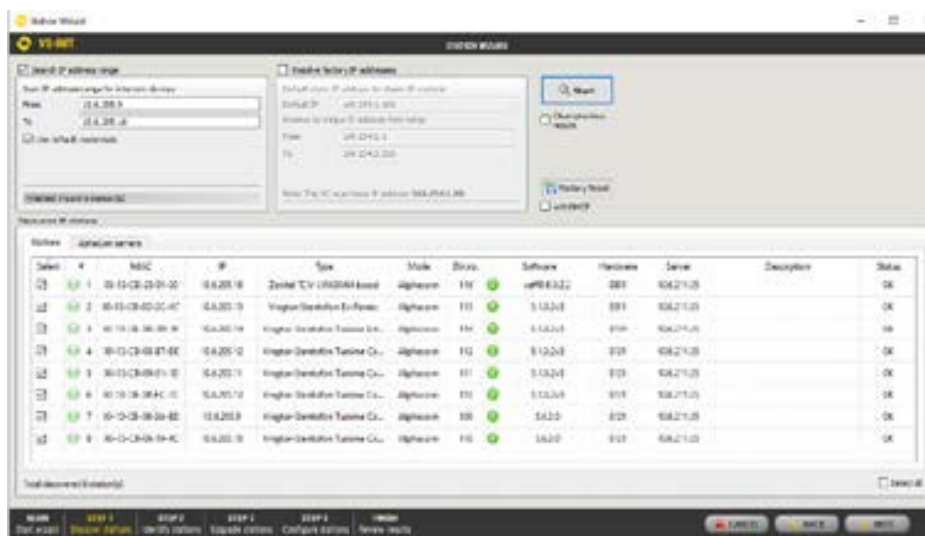
Installation et configuration de dispositifs d'interphonie IP pour la cybersécurité

Voici les étapes de base pour mettre en place le système, en utilisant l'IMT pour les paramètres affectant la cybersécurité :

2.

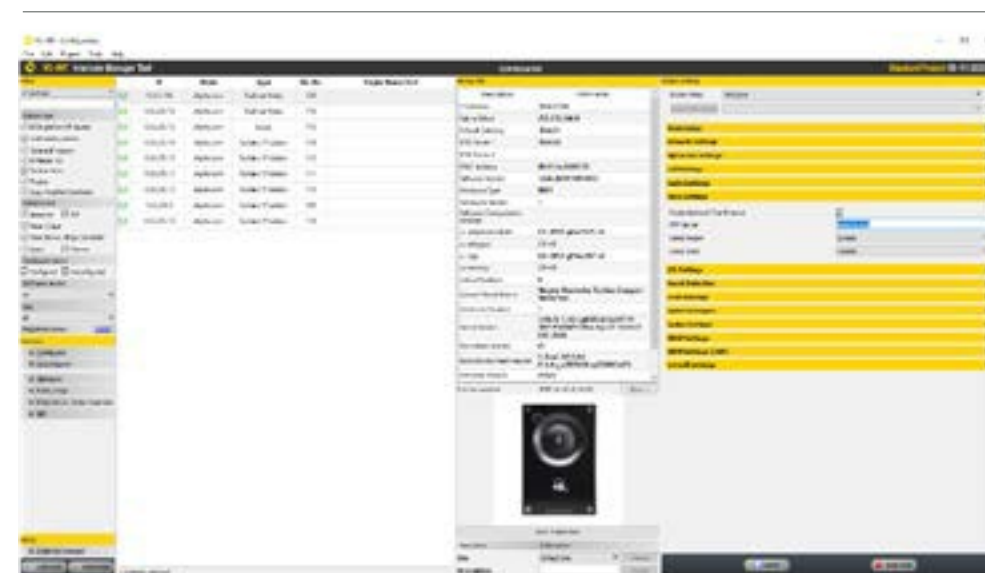
1. Lancez l'IMT et découvrez les postes.

- Démarrez l'outil PC VS-IMT.
- Ouvrez la base de données des projets existants ou appuyez sur Créer pour faire un nouveau projet.
- Appuyez sur **File > Launch Station Wizard** et **Enter**.
- Sélectionnez **Rechercher (Search)**, et l'IMT trouvera toutes les unités Zenitel.



Changez le mot de passe par défaut pour l'accès admin pour toutes les stations.

- Appuyez sur *Suivant (Next)* jusqu'à parvenir à la page de configuration des postes.
- Sélectionnez tous les postes (Ctrl+ A), Saisissez le nouveau mot de passe, puis Chargez (**Upload**).
- Appuyez deux fois sur *Suivant* pour terminer l'assistant de poste.



3. Définissez le serveur NTP pour tous les postes.

- Dans la page de configuration, sélectionnez tous les postes (Ctrl + A) et ouvrez les paramètres de temps (**Time Settings**).
- Activez le protocole de temps réseau et saisissez un nom d'hôte ou une adresse IP valide pour le serveur NTP.
- Appuyez sur Enregistrer (**Save**), puis sur Télécharger (**Upload**)



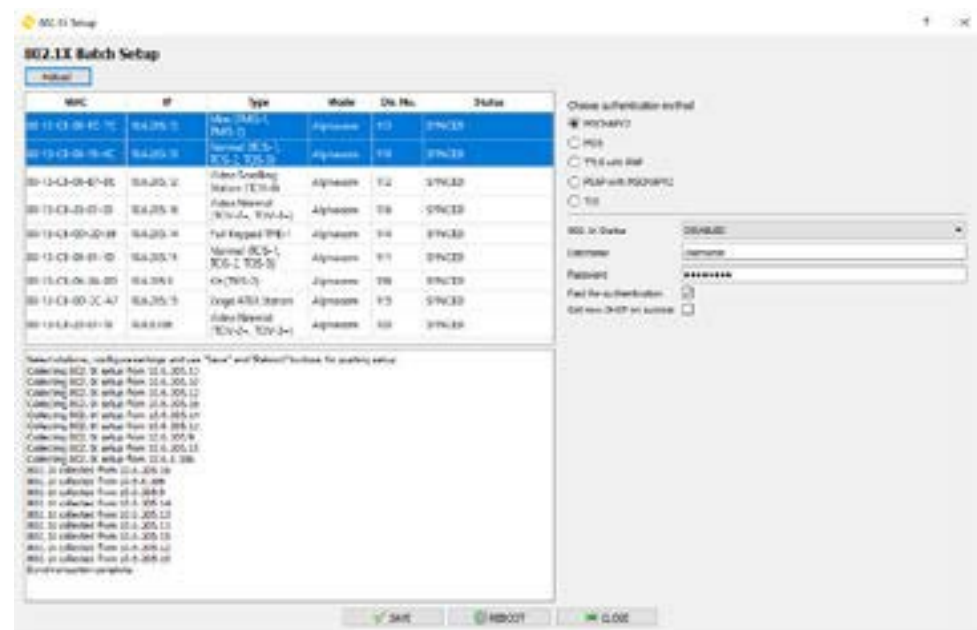
4. Définissez les paramètres SNMP

- Dans la page Configuration, sélectionnez toutes les stations (Ctrl + A) et ouvrez Paramètres SNMP.
- Saisissez les paramètres SNMP pertinents.
- Appuyez sur Enregistrer (**Save**), puis sur Télécharger (**Upload**)



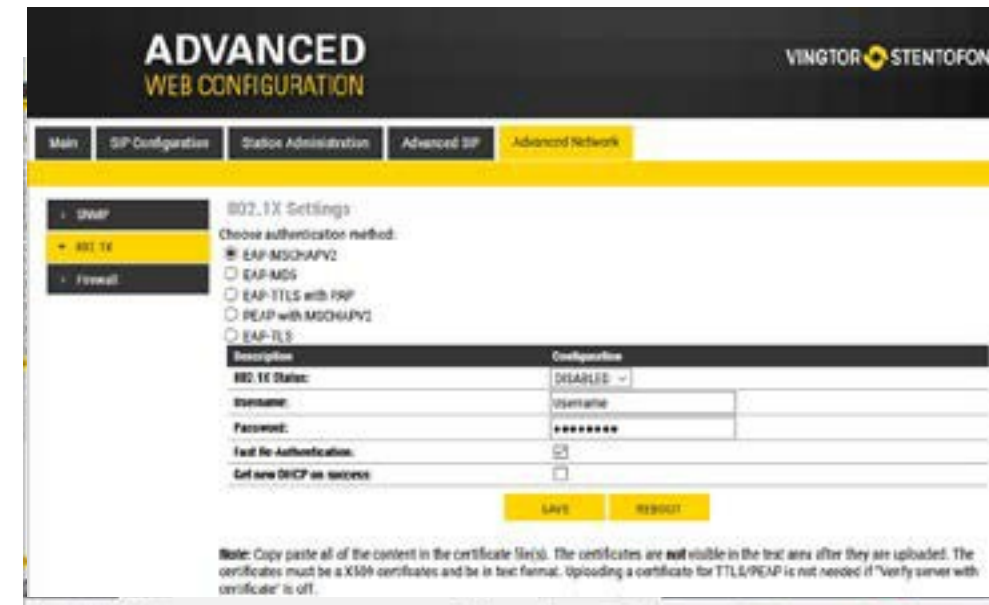
5. Activez IEEE802.1x et définissez les paramètres d'authentification.

- Sur la page de configuration (**Configuration page**), dans la barre de menu, sélectionnez Outils (**Tools**) > Configuration 802.1X (**802.1X Setup**). Sélectionnez tous les postes (Ctrl + A).
- Saisissez les paramètres d'authentification pertinents.
- Appuyez sur Enregistrer (**Save**), puis sur Redémarrer, (**Reboot**).



5a. IEEE802.1x au niveau de l'appareil final

- Connectez-vous à la page de configuration Web à bord de l'appareil.
- Ouvrez l'onglet Réseau avancé. (**Advanced Network**)
- Sélectionnez la méthode d'authentification souhaitée.
- Cliquez sur Enregistrer (**Save**), puis sur Redémarrer (**Reboot**).



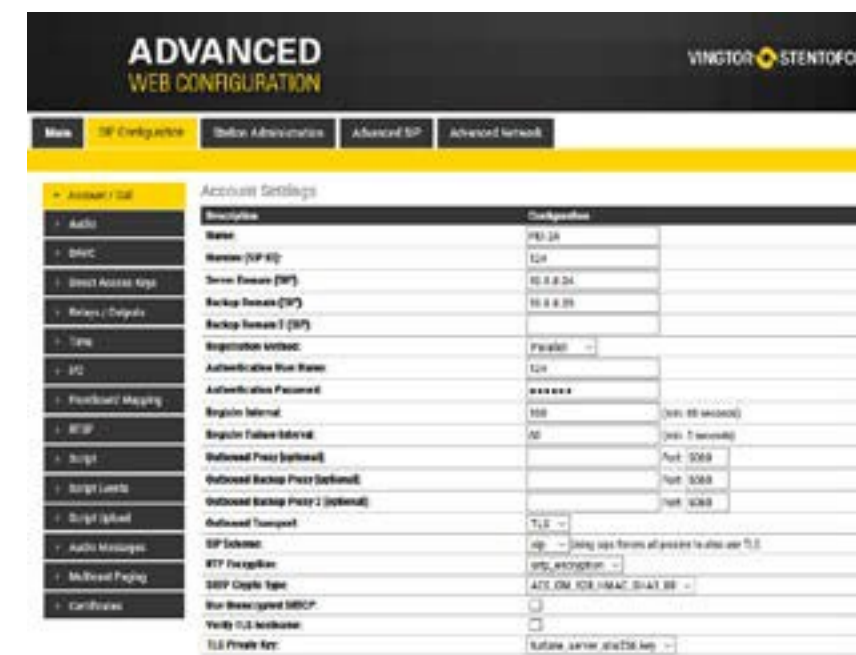
6. Vérifiez les ports IP et les paramètres du pare-feu.

- Sur la **Configuration page**, sélectionnez un poste.
- Ouvrez le Pare-feu (**Firewall**)
- Vérifiez que les services autorisés/bloqués sont définis en fonction des services nécessaires.
- Vérifiez les paramètres du pare-feu pour chaque poste.



7. Générez un rapport de description du système.

- Lancez l'Assistant de poste. en sélectionnant Fichier **File** > Lancer l'Assistant de Station **Launch Station Wizard** et exécutez le processus de découverte de poste .
- À partir de la dernière étape de l'Assistant, utilisez le générateur de rapports pour créer un rapport système.



8. Configurez la sécurité en mode SIP (au niveau de l'appareil final)

- Connectez-vous à la page de configuration Web à bord de l'appareil.
- Accédez à l'onglet Configuration SIP (**SIP configuration**) et à la section Compte/Appel (**Account/Call**)
- SIP over TLS crypte la couche de transport en utilisant la même méthode que HTTPS.
- TLS 1.2 est pris en charge.
- Le cryptage SRTP est également pris en charge dans les formats suivants : AES_CM_128HMAC_SHA1_80 AES_CM_128HMAC_SHA1_32
- Les fonctions peuvent également être configurées dans l'IMT.
- NB : Actuellement non supporté sur TCIV+.

ALPHA
COM XE

ICX-AlphaCom



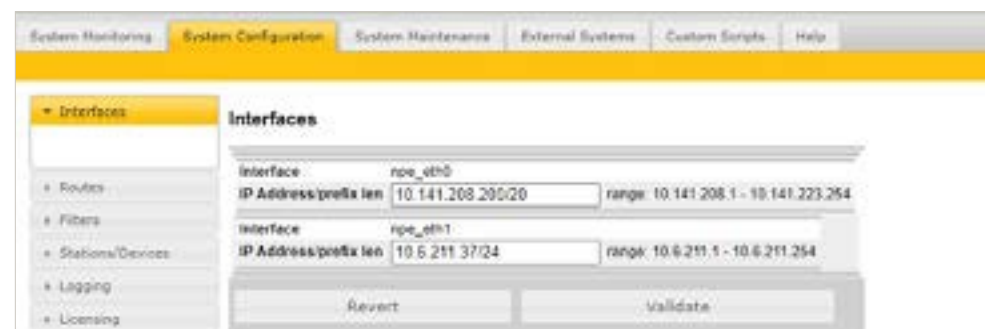
Installation et configuration du serveur ICX 500 & ICX-AlphaCom / AlphaCom XE pour la cybersécurité

Voici les étapes de base pour configurer le système en utilisant l'interface web ICX-AlphaCom / AlphaCom pour les paramètres liés à la cybersécurité :



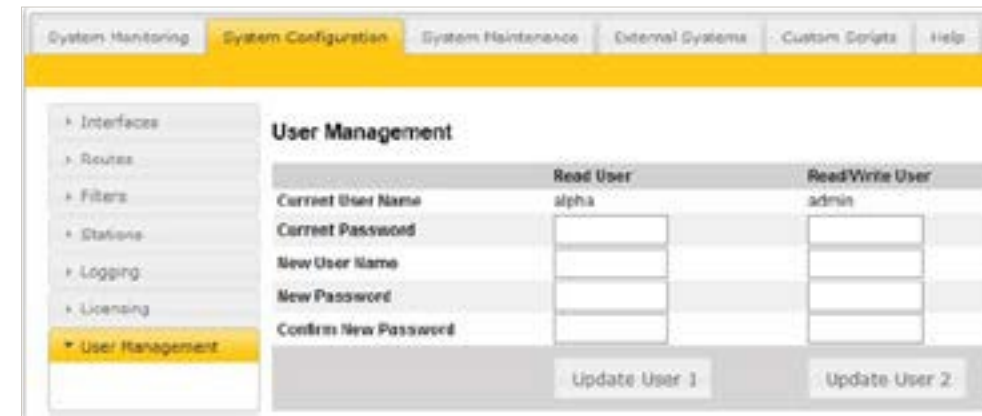
1. Connectez-vous à AlphaWeb.

Vous pouvez vous connecter via le protocole HTTP ou le protocole sécurisé HTTPS.



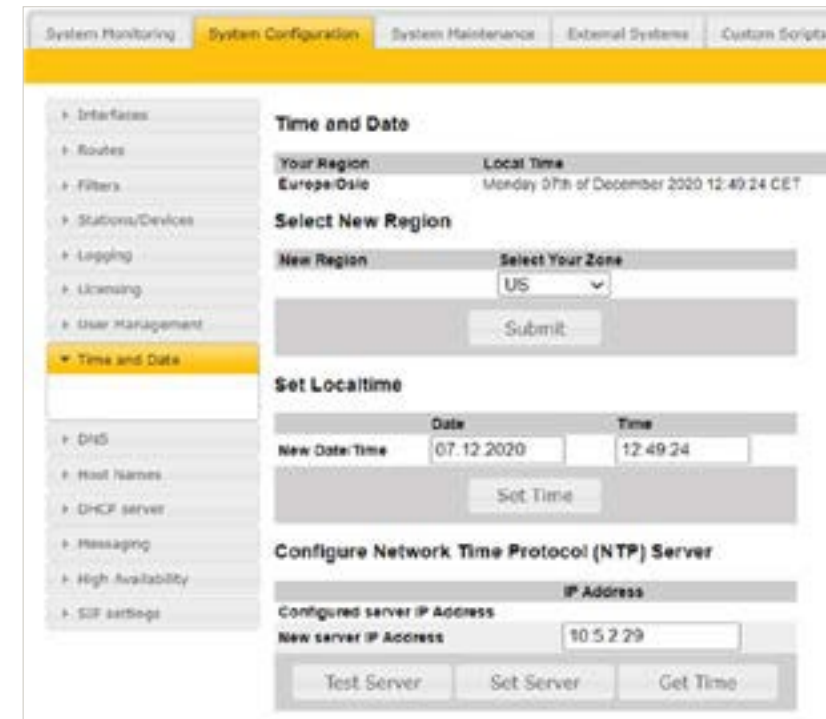
2. Définissez la configuration IP.

L'ICX-AlphaCom / AlphaCom possède deux interfaces Ethernet. Par défaut, un port est utilisé pour le trafic VoIP, l'autre pour la gestion.



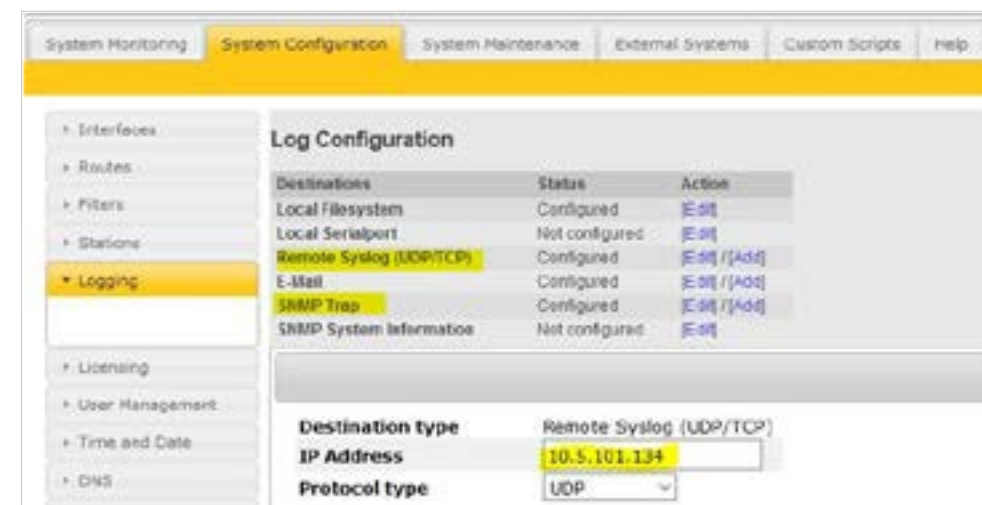
3. Modifiez le mot de passe par défaut.

Il existe deux types de mots de passe : un pour l'accès en lecture seulement et un pour l'accès en lecture/écriture.

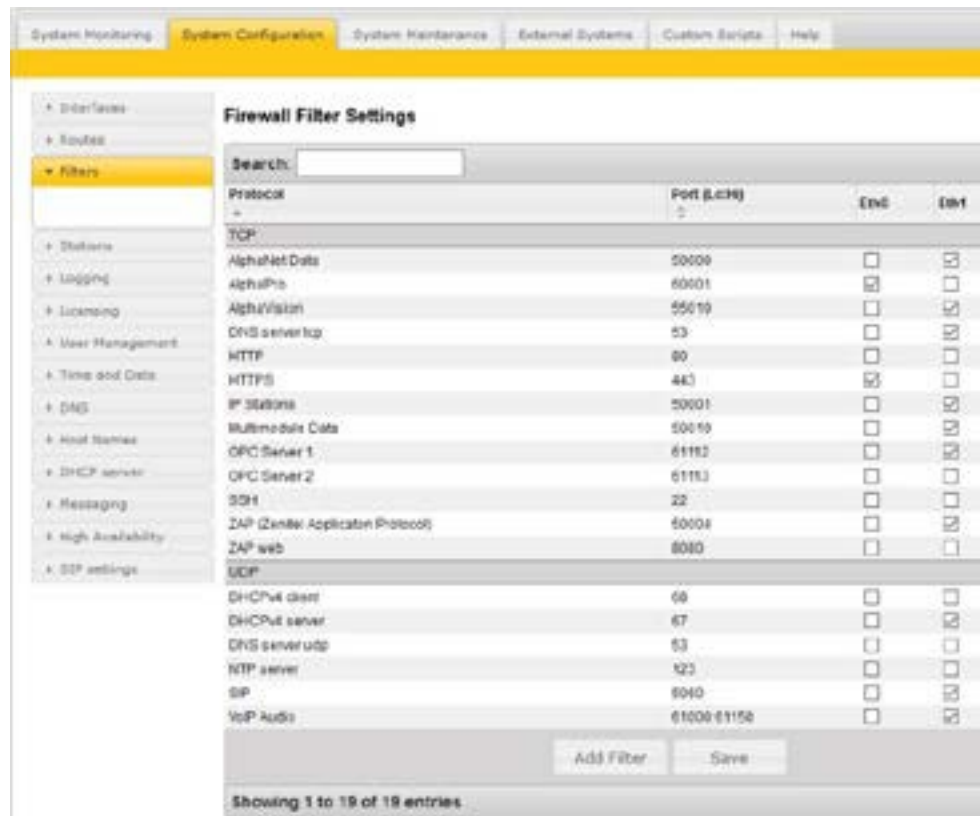


4. Définissez le serveur NTP.

L'ICX-AlphaCom / AlphaCom peut synchroniser son horloge à partir d'un serveur NTP.



5. Activez les trappes SNMP et/ou Syslog pour la surveillance..



6. Vérifiez les ports IP et les paramètres du pare-feu.

Assurez-vous que tous les ports inutilisés sont désactivés.

L'AlphaPro prend en charge le HTTPS (port 443).



ICX-500

8. Pour ICX uniquement, Configurer l'IP à haute disponibilité IP:

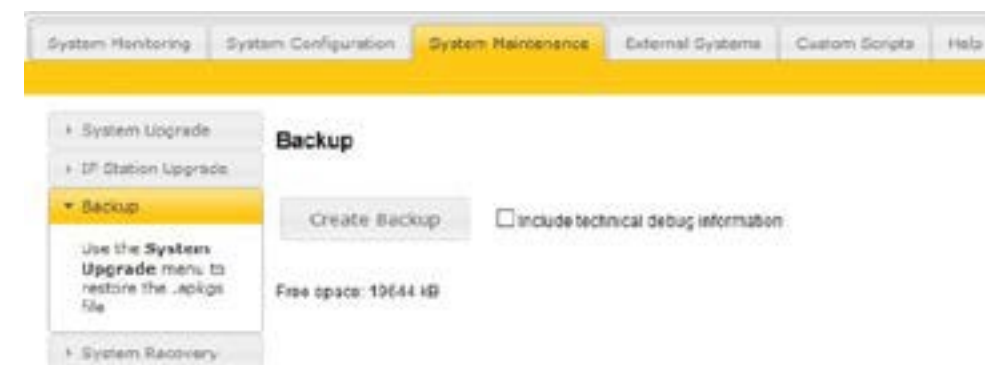
- Configurez à partir de Configuration du système (**System configuration**) -> Haute disponibilité (**High availability**).
- Cochez la case pour TLS/HTTPS (443).
- Cliquez sur Valider (**Validate**).



ICX-500

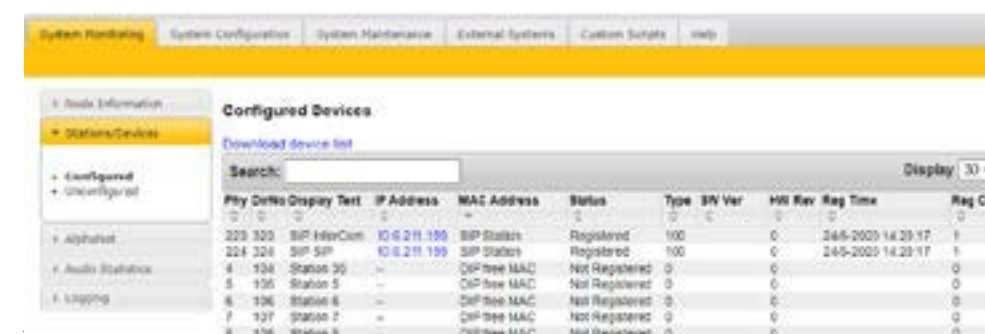
7. Pour ICX uniquement, configurer 802.1x.

- Configurez à partir de Configuration du système -> 802.1x.
- Sélectionnez la méthode d'authentification souhaitée.
- Cliquez sur Appliquer (**Apply**)



9. Sauvegardez les données de configuration.

Les données de configuration sont stockées dans un fichier local sur le serveur, ainsi que sur le PC externe.



10. Générez un rapport de description du système.

Vous pouvez générer un rapport Microsoft Excel contenant tous les dispositifs configurés.

CONTRÔLER

REEMPLIR LA LISTE DE VÉRIFICATION DU SYSTÈME DE CYBERSÉCURITÉ

Après avoir terminé la phase de mise en œuvre pour assurer la cybersécurité de votre système, il est temps de vérifier comment les choses se passent. Pour vous aider à démarrer, nous avons compilé une liste de contrôle simple reliant les tâches nécessaires aux contrôles CIS pertinents.

ID DE CONTRÔLE CIS	TÂCHE	OBJECTIF	CONSTATATIONS
Contrôle CIS 1 : inventaire et contrôle des biens matériels	Examinez les registres des dispositifs autorisés ayant accédé au réseau.	Vérifiez que les interphones autorisés n'ont pas de déconnexions non planifiées du réseau.	
		Vérifiez qu'aucun dispositif inconnu n'a accédé au réseau utilisé pour la sécurité physique.	
Contrôle CIS 2 : inventaire et contrôle des actifs logiciels	Vérifiez la version du logiciel de vos appareils d'interphonie	Vérifiez que vous disposez du dernier logiciel de production sur les appareils d'intercom Zenitel. Voir les notes de version sur wiki.zenitel.com .	
Contrôle CIS 3 : gestion continue des vulnérabilités	Vérifiez quand le mot de passe de connexion a été modifié pour la dernière fois	"Évaluez la nécessité de changer le mot de passe, conformément à la politique de l'entreprise. Il ne devrait pas y avoir de résultats critiques de l'analyse de vulnérabilité »	
Contrôle CIS 4 : utilisation contrôlée des privilèges administratifs	Effectuez un scan de vulnérabilité sur le réseau de sécurité physique	Seuls les administrateurs actuels doivent connaître les mots de passe actuels de l'administrateur.	
Contrôle CIS 6 : maintenance, surveillance et analyse des journaux d'audit	Vérifiez qui a accès aux mots de passe d'administration des dispositifs de sécurité physique.	Vérifiez que les interphones autorisés n'ont pas de déconnexions non planifiées du réseau/serveur.	
Contrôle CIS 9 : limitation et contrôle des ports, protocoles et services du réseau.	Examinez les rapports SNMP et syslog	Vérifiez qu'aucun port pour des services non utilisés n'est ouvert.	



AGIR

ÉVALUER ET ASSURER LE SUIVI

Une fois que vous aurez complété la liste de contrôle de cybersécurité à l'étape précédente, vous disposerez d'une série de résultats qui façonneront votre plan d'action pour tout suivi nécessaire. Passez en revue les conclusions de la liste de contrôle et identifiez les actions nécessaires pour chacune d'elles. Admettons par exemple que votre constatation concernant le contrôle 4 du CIS est la suivante:

ID DE CONTRÔLE CIS	TÂCHE	OBJECTIF	CONSTATATIONS
Contrôle CIS 4 : utilisation contrôlée des privilèges administratifs	Vérifiez qui a accès aux mots de passe d'administration des dispositifs de sécurité physique.	Seuls les administrateurs actuels connaissent les mots de passe actuels des administrateurs.	Certains anciens administrateurs ont les mots de passe actuels des administrateurs.

Naturellement, l'action de suivi requise est de changer immédiatement vos mots de passe d'administrateur.

Une fois que vous aurez identifié toutes les actions de suivi, vous pourrez plus facilement les classer par ordre de priorité, évaluer les besoins en ressources et les mener à bien.

La collecte de ces informations de manière structurée et cohérente simplifiera le suivi et vous permettra de rendre compte régulièrement à la direction de la santé de votre système en matière de cybersécurité.

Nous espérons que ce guide vous aidera à faire face à vos risques de cybersécurité et à vous assurer que vous maintenez une cyberdéfense saine et solide pour vos systèmes.

POUR EN APPRENDRE PLUS



TÉLÉCHARGER

Notre progiciel et notre logiciel sont disponibles via nos pages :

<https://www.zenitel.com/customer-service/wiki-access>



INFORMATIONS GÉNÉRALES

Nous concevons chacune de nos solutions dès le départ en tenant compte de la défendabilité:

<https://www.zenitel.com/cybersecurity/vingtor-stentofon-cybersecurity>



Le **CIS** (Center for Internet Security) est une organisation indépendante à but non lucratif dont la mission est de fournir une expérience en ligne sécurisée pour tous:

<https://www.cisecurity.org>



SERVICE CLIENT

Nous sommes disponibles pour prendre votre demande :

Téléphone : 01 47 88 50 00

Email: zenitel.france@zenitel.com

www.zenitel.fr